Universidad Politécnica de Cataluña

Facultad de Matemáticas y Estadística

Trabajo de fin de grado

BINARY QUADRATIC FORMS

Cassius Manuel Pérez de los Cobos Hermosa

Director: Jordi Quer Bosor

I

Forse altro canterà con miglior plectro

Orlando Furioso, XXX, 16

Contents

Introduction

The early questions asked about forms were all related to the representation of integers. Although there are many ways to state a problem of this kind, the most common one was to characterize all numbers represented by a given form $f(x, y)$. The most well-known examples are those when the given form is $f(x, y) = x^2 + y^2$, first solved by Euler around 1750, and Pell's equation $x^2 - Dy^2 = 1$, which was known since ancient times but whose detailed description was not compiled until 1769 by Lagrange. Legendre was the first one who sought to study quadratic binary forms not only in particular cases but trying to elaborate a more general theory. However, the publication of *Disquisitiones Arithmeticae* by Gauss in 1801 would undoubtedly give birth not only to the theory of forms, but to Number Theory as a coherent field of mathematics. The most relevant technique he introduced was the composition of forms (in a surprising exhibition of computational skill) in a context where the notion of group was not clear yet.

This work is divided into two parts. The first one is nothing but a rephrasing of the fifth section of *Disquisitiones Arithmeticae*. Notationally speaking, the biggest difference is that our definition of form is that of Eisenstein allowing the coefficient in xy to be odd, while Gauss's considers only forms $f(x, y) = ax^2 + 2bxy + y^2$, with determinant $b^2 - ac$. Each convention has its complications, but ours is the one used in modern theories, principally because the forms of Eisenstein's definition correspond with all the class groups of quadratic number fields, unlike Gauss's.

The text we have used the most in this part is Buell's *Binary Quadratic Forms* [2], although at some points it lacks formality and we preferred Mathews' [3] or even the *Disquisitiones* [1], even though it is necessary to deal with their antiquate notation. In any case we strongly recommend the reader to visit Gauss's at least once in order to understand the landmark it meant in the history of mathematics.

In the second part we tried to adapt the theory if, instead of in the integers, the coefficients of the forms live in $\mathbb{F}_q[T]$, the ring of polynomials

with coefficients in a finite field with characteristic distinct from two. Since $\mathbb{Z}$ and $\mathbb{F}_q[T]$ are both euclidean, these two theories share many properties, although at some points their behavior differs. Not too much literature has been dedicated to this matter, so the only work we have been supported by was Enric Meinhardt's bachelor thesis, which gave us the necessary ideas to create a more detailed description. The chapter dedicated to the real case is completely original, so we are responsible of its virtues and lacks. Between the latter, the most significant one is that we could not completely prove that the equivalence between two forms implies that they belong to the same cycle. This absence is due to our incapability to control the sign of the partial quotients in the expression of the principal root of a form as a simple continued fraction, in contrast to what we did manage to solve in the integers.

Part I

Forms with coefficients in $\mathbb{Z}$

Chapter 1

Preamble

This chapter contains all the results not necessarily related to the theory of binary forms.

1.1 Continued Fractions

Since continued fractions in $\mathbb{R}$ are a well known topic, we will settle for setting clearly the notation and properties we will need, without proving most of them. A detailed description can be found in [4], and a more brief one in [2].

Definition 1.1. *A finite continued fraction is an expression*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_N}}}$$

provided it is defined, where all $a_i \in \mathbb{R}$.

We will more briefly write this expression as $[a_0; \cdots, a_N]$, separating the first term from the rest with a semicolon. If $a = [a_0; \cdots, a_N]$ we will say this is an expression of a as a continued fraction, or alternatively that it represents a. The a_i are the *partial quotients* of the continued fraction. The *n-th convergent* of this expansion is defined as

$$R_n = [a_0; \cdots, a_n], 0 \leq n \leq N,$$

provided we do not divide by zero. Otherwise it is undefined.

We also define

$$P_{-1} := 1; \quad P_0 := a_0; \quad P_n := a_n P_{n-1} + P_{n-2} \text{ for } n \geq 1$$

and

$$Q_{-1} := 0; \quad Q_0 := 1; \quad Q_n := a_n Q_{n-1} + Q_{n-2} \text{ for } n \geq 1.$$

We have the following result, easy to prove by induction:

Proposition 1.2. *The following identities hold*

1. $R_n := [a_0; \cdots, a_n] = \frac{P_n}{Q_n}$ *for* $n \geq 0$.
2. $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$, *for* $n \geq 0$.
3. $\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_{n-1} Q_n}$ *for* $n \geq 0$.

Definition 1.3. *A finite simple continued fraction (finite scf) is a finite continued fraction* $[a_0; \cdots a_N]$ *where* $a_0 \in \mathbb{Z}$ *and* $a_n \in \mathbb{N} = \{1, 2, \cdots\}$ *for every* $n \in [1, N]$.

Any finite scf represents a rational number, and conversely every rational number is represented by a finite scf. A rational number has exactly two expressions as a finite scf, one where the last partial quotient is 1 and another one where the last quotient is greater than 1, since we have $[z] = [z - 1, 1]$. Unless otherwise stated we will be forcing the last quotient to satisfy $a_N > 1$, so we will say the representation of a rational number as a finite scf is unique or essentially unique.

Proposition 1.2 allows us to define an infinite scf by considering the limit of a sequence of finite scf's (which exists, although we do not give a proof). More formally, we have the following definition:

Definition 1.4. *Given* $\{a_i\}_{i \in \mathbb{N}_0}$ *where* $a_0 \in \mathbb{Z}$ *and* $\forall n \in \mathbb{N}$, $a_n \in \mathbb{N}$, *an infinite simple continued fraction (infinite scf) is a notational expression* $[a_0; a_1, \cdots]$ *whose value equals the limit*

$$\lim_{n \to \infty} R_n,$$

where $R_n = [a_0; \cdots, a_n]$.

Infinite scf's are strictly unique: if $[a_0; a_1, \cdots] = [b_0; b_1, \cdots]$, then all quotients are identical since $[0; a_n, a_{n+1}, \cdots] < 1$ for any $n \in \mathbb{N}$.

Every infinite scf converges to a real number. Conversely, if we are given a real number x, then the following algorithm gives us its expression as a (finite or infinite) scf:

We define a_i, X_i, Z_i as

$$a_0 = \lfloor x \rfloor; \quad Z_0 = x - a_0,$$

$$X_i = \frac{1}{Z_{i-1}}; \quad a_i = \lfloor X_i \rfloor; \quad Z_i = X_i - a_i; \quad i \geq 1$$

The algorithm continues as long as $Z_i \neq 0$. The a_i's satisfy $x = [a_0; \cdots a_{i-1}, X_i]$, where X_i is not necessarily an integer.

If $x \in \mathbb{Q}$, then the algorithm is actually a rephrasing of the classical euclidean algorithm applied to the numerator and the denominator, therefore eventually it finishes.

If x is irrational, then the succession $(R_n)_{n \in \mathbb{N}_0}$ converges to x, hence $[a_0; a_1, \cdots]$ is the scf of x.

Since under the stated conventions every real number has an unique scf, we will identify scf's with real numbers without further explanations.

In general we will only consider scf's of the following type:

Definition 1.5. *The infinite scf* $[a_0; a_1 \cdots]$ *is called* periodic *(of period* p*) if there exist integers* $I \geq 0$ *and* $p \geq 1$ *so that* $a_i = a_{i+p}$ *for all* $i \geq I$*, and we will write*

$$x = [a_0; \cdots a_{I-1}, *a_I, \cdots, *a_{I+p-1}],$$

where the $*$ *indicates the period. We will also refer to the ordered set* $\{a_I, \cdots, a_{I+p-1}\}$ *as the* period *of the periodic scf.*

If $a_0 = 0$ *and* $I = 1$*, we will say the scf is pure periodic.*

Periodic scf's can be characterized as quadratic irrationals, i.e. those $x \in \mathbb{R} \setminus \mathbb{Q}$ such that they satisfy $ax^2 + bx + c = 0$, where $a, b, c \in Z$. Note that, since $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$, it will be necessary that $b^2 - 4ac$ is not a square and positive. We will give a proof of this fact later with the appropriate tools.

We will also need the two following results:

Proposition 1.6. *If a continued fraction has only integer partial quotients and only a limited number of them are negative or zero, then it is possible, by a finite number of steps, to convert it into a scf.*

Proof. Let $[a_1; a_2, \cdots]$ be the continued fraction. Let a_r be the last partial quotient which is not positive. There are different cases:

1. $a_r = 0$. We have the identity $[a; 0, b, x] = [a + b; x]$, hence we can do

$$[\cdots, a_{r-1}, 0, a_{r+1}, a_{r+2}, \cdots] = [\cdots, a_{r-1} + a_{r+1}, a_{r+2}, \cdots],$$

   leaving the rest unaltered.

2. $a_r = -n$ with $n > 1$. We have the identity $[a; -b, x] = [a - 1; 1, b - 2, 1, x - 1]$, so we can do

$$[\cdots, a_{r-1}, -n, a_{r+1}, \cdots] = [\cdots, a_{r-1} - 1, 1, n - 2, 1, a_{r+1} - 1, \cdots],$$

   where $a_{r-1} - 1$ is the only quotient which could be negative. If either $n - 2$ or $a_{r+1} - 1$ is zero, we can apply the procedure of the previous case.

3. $a_r = -1$ and $a_{r+1} > 1$. We have the identity $[a; -1, x] = [a-2; 1, x-2]$, hence we can write

$$[\cdots, a_{r-1}, -1, a_{r+1}, \cdots] = [\cdots, a_{r-1} - 2, 1, a_{r+1} - 2, \cdots],$$

   where $a_{r-1} - 2$ is the only quotient which could be negative.If $a_{r+1} - 2$ is zero the first reduction may be applied.

4. $a_r = -1$ and $a_{r+1} = 1$. We have the identity $[a; -1, 1, b, x] = [a - b - 2; 1, x - 1]$, so we can replace

$$[\cdots, a_{r-1}, -1, 1, a_{r+2}, a_{r+3}, \cdots] = [\cdots, a_{r-1} - a_{r+2} - 2, 1, a_{r+3} - 1, \cdots],$$

   where $a_{r-1} - a_{r+2} - 2$ is the only quotient which could be negative. If $a_{r+3} - 1$, then we can apply the first reduction.

In every case the last negative quotient is brought at least one place nearer to the beginning of the fraction. Therefore, after a finite number of steps, the continued fraction becomes a scf, as desired.

□

There is a notorious fact about last demonstration. Each stated reduction leaves the position of the partial quotients unaltered or increases or decreases it by two. Therefore the quotients will occupy places in the scf expansion with the same parity of the original continued fraction. This fact will be invoked later.

Proposition 1.7. *Let $x, y \in \mathbb{R}$. If there exist integers $\alpha, \beta, \gamma, \delta$ so that $\alpha\delta - \beta\gamma = 1$ and*

$$y = \frac{\alpha x + \beta}{\gamma x + \delta},$$

then we can express y as

$$y = [u; a_1, \cdots, a_{2r}, v, x],$$

where $a_1, \cdots, a_{2r}$ are positive integers and u, v are integers.

Proof. If β or γ are zero, the result is obvious. Otherwise let u be defined as $u := \lfloor \beta/\delta \rfloor$, so $\beta/\delta - u$ is a positive proper fraction. We can expand $\beta/\delta - u$ into a scf, and if it happens that the number of partial quotients is odd, then using that $[z] = [z - 1, 1]$, we can increase their number by one. After this, we have

$$\frac{\beta}{\delta} = [u; a_1, \cdots, a_{2r}].$$

Now suppose P/Q is the penultimate convergent of this scf. Then, by the properties of proposition 1.2, we have

$$\beta Q - \delta P = 1 = \alpha\delta - \beta\gamma.$$

In other words, we have the solutions $(x, y) = (Q, P)$ and $(x, y) = (-\gamma, \alpha)$ of the Diophantine equation $\beta x - \delta y = 1$. Therefore this two solutions must satisfy

$$\alpha = P + v\beta; \quad \gamma = Q + v\delta$$

for some integer v. Using again proposition 1.2,

$$\alpha/\gamma = [u; a_1, \cdots, a_{2r}, v],$$

and applying it one more time, we finally deduce

$$y = \frac{\alpha x + \beta}{\gamma x + \delta} = [u; a_1, \cdots, a_{2r}, v, x],$$

as we wanted to prove.

□

1.2 The modular group

Definition 1.8. *The group $SL(2,\mathbb{Z})$ is the multiplicative group of the 2×2-matrices with coefficients in $\mathbb{Z}$ and determinant 1.*

Two important elements of $SL(2,\mathbb{Z})$ are the matrices

$$S := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \quad T := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

as the following proposition corroborates.

Proposition 1.9. *The group $SL(2,\mathbb{Z})$ can be generated by its elements S and T. In other words, any matrix $M \in SL(2,\mathbb{Z})$ can be written as*

$$S^{i_1}T^{j_1}S^{i_2}\dots S^{i_k}T^{j_k},$$

being all the exponents integers.

Proof. First of all, we note that

$$S^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Moreover,

$$S^{-n} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.$$

Since $T^2 = -\mathrm{Id}$, the order of T in $SL(2,\mathbb{Z})$ is 4.

Let $M \in SL(2,\mathbb{Z})$. In order to prove the proposition, it is enough to multiply it on the left by S and T until we obtain the identity.
We consider the matrices M, TM, T^2M, T^3M. Since no matrix in $SL(2,\mathbb{Z})$ can contain a column of zeros, one of them four must be a matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

so that $\beta > 0$ and $\beta \geq |\delta|$. In case δ is not zero, we multiply on the left by S^n and get

$$\begin{pmatrix} \alpha + n\gamma & \beta + n\delta \\ \gamma & \delta \end{pmatrix}.$$

We choose an adequate n so that $|\delta| > \beta + n\delta \geq 0$. Repeating these process, by infinite descent, we eventually obtain a matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

with β or δ equal zero. Multiplying by T if necessary, we can say $\beta = 0$. Since its determinant is 1, it satisfies $\alpha = \delta = \pm 1$. Multiplying by T^2 if necessary, it has the form

$$\begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}.$$

Now, since

$$T^3 S^\gamma T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\gamma & 1 \end{pmatrix},$$

multiplying on the left by $T^3 S^\gamma T$, we finally obtain the identity, as desired.

□

Chapter 2

First steps

A quadratic binary form with integer coefficients, or more briefly from now on a form, is an homogeneous polynomial

$$f(x, y) = ax^2 + bxy + cy^2$$

where a, b, c are integers. In these conditions, when the values of the variables are not taken into account, the form $f(x, y)$ will be denoted when convenient as the ordered set (a, b, c).

The forms such that $\gcd(a, b, c) = 1$ are called *primitive* forms. We will limit our work to these forms, for the properties of non primitive forms can be easily deduced from them. When working with those ones, $\gcd(a, b, c)$ is normally referred as the *multiplier* of the form.

Definition 2.1. *The discriminant D of the form (a, b, c) is $D = b^2 - 4ac$.*

Note that the discriminant must satisfy $D \equiv 1 \pmod 4$ or $D \equiv 0 \pmod 4$. Reciprocally, given any integer $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$, there exist primitive binary forms with that discriminant. For example we can consider

- $I_D = (1, 0, -D/4)$ if $D \equiv 0 \pmod 4$
- $I_D = (1, 1, \dfrac{1 - D}{4})$ if $D \equiv 1 \pmod 4$.

This is called the *principal form* with discriminant D.

2.1 Transformations between forms

Suppose we are given the forms

$$f := f(x, y) = ax^2 + bxy + cy^2$$

with discriminant D and

$$f' := f'(x', y') = a'x'^2 + 2b'x'y' + c'y'^2$$

with discriminant D'.

The *matrix of* f is

$$A_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

As we can see, the matrix A_f is symmetric with integer coefficients, except the elements of its anti-diagonal, which can be half-integers. It satisfies $D = -4 \det A_f$, and we can write

$$f = \begin{pmatrix} x & y \end{pmatrix} A_f \begin{pmatrix} x \\ y \end{pmatrix}.$$

We recall that in the preamble the group $SL(2, \mathbb{Z})$ was defined as the multiplicative group of the 2×2-matrices with coefficients in $\mathbb{Z}$ and determinant 1.

Definition 2.2. *The forms f and f' are* equivalent *(by means of the matrix M) if there exists a matrix $M \in SL(2, \mathbb{Z})$ such that $M^T A_f M = A_{f'}$, what we will write as $f \sim f'$. In this case we define $f|_M := f'$.*

The relation "$\sim$" is obviously symmetric and reflexive. If $M^T A_g M = A_f$ and ${M'}^T A_h M' = A_g$, then

$$A_f = M^T {M'}^T A_h M' M = (MM')^T A_h MM',$$

so since the matrix MM' also has determinant 1, we deduce $f \sim h$, which means that this relation is also transitive. All in all, this is a true equivalence relation.

The importance of the determinant comes from its invariance through equivalent classes. If $f|_M = f'$, we have

$$\det A_f = \det M^t A_{f'} M = (\det M)^2 \det A_{f'} = \det A_{f'},$$

so since $D = -4 \det A_f$, this implies $D = D'$. The reciprocal does not hold, which encourages us to state the following definition:

Definition 2.3. *The set of equivalence classes under the relation "$\sim$" is denoted as $Cl(D)$.*

The set $Cl(D)$ is actually a group under a very natural operation, so it is normally referred as *the class group.* Later we will prove this fact.

Given $D \in \mathbb{Z}$, the group $SL(2,\mathbb{Z})$ acts on the right on the set of forms of discriminant D. The action of M on a form with matrix A_f produces a form $f|_M$ with matrix $M^T A_f M$. The orbits of this action are the classes of forms under the equivalence relation "$\sim$", or differently explained, the set of orbits is $Cl(D)$.

Since M and $-M$ act identically on a form f, in order to identify them we define the modular group as

$$PSL(2,A) := SL(2,A)/\{\pm \mathrm{Id}\},$$

which is the one we will use from now on. Therefore the transformations matrices will be considered as matrices whose sign may change conveniently.

Note that the discriminant is also invariant if we allow the matrices M to have determinant -1. When $\det M = -1$ and $f|_M = f'$, we will say that f and f' are *improperly equivalent.* However, this is not an equivalence relation.

The definition of equivalence is based on the equivalent changes of variables (also called transformations). If $f|_M = f'$, being

$$M := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2,\mathbb{Z}),$$

then through the transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix},$$

we get

$$f(x,y) = \begin{pmatrix} x' & y' \end{pmatrix} M^T A_f M \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x' & y' \end{pmatrix} A_{f'} \begin{pmatrix} x' \\ y' \end{pmatrix} = f(x',y').$$

Thus we can state that f and f' are equivalent iff there exist $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ so that $\alpha\delta - \beta\gamma = 1$ and

$$f(\alpha x + \beta y, \gamma x + \delta y) = f'(x,y),$$

what we can rewrite as

$$f(\alpha,\gamma)x^2 + [b(\alpha\delta+\beta\gamma) + 2(a\alpha\beta + c\gamma\delta)]xy + f(\beta,\delta)y^2 = f'(x,y).$$

We have the following equations, which we will refer as *equivalence equations*:

$$\begin{aligned} a\alpha^2 + b\alpha\gamma + c\gamma^2 &= a' \\ b(\alpha\delta+\beta\gamma) + 2(a\alpha\beta + c\gamma\delta) &= b' \\ a\beta^2 + b\beta\delta + c\delta^2 &= c' \end{aligned} \tag{2.1}$$

2.2 Useful equivalences

As we proved in the preamble, the group $SL(2,\mathbb{Z})$ is generated by its elements S and T defined as

$$S := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};\ T := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

These matrices act as follows on a form $f = (a,b,c)$:

- $f|_{S^k} = (a, b+2ak, ak^2+bk+c)$
- $f|_T = (c,-b,a)$

The first one of these actions implies that (a,b,c) and (a,b',c') are equivalent provided they share discriminant and $b \equiv b' \pmod{2a}$.

But we will also need the following equivalences:

Doing $x = y'$ and $y = x'$, we see that (a,b,c) and (c,b,a) are improperly equivalent. We will say (c,b,a) is the *associated form* of (a,b,c).

By applying T to (c,b,a) and using last result we see the forms (a,b,c) and $(a,-b,c)$ are improperly equivalent. We say these two forms are *opposed*.

Definition 2.4. *The forms $f = (a,b,c)$ and $f' = (a',b',c')$ are* adjacent*, or more precisely the form f' is right adjacent to the form f, if they satisfy the following three properties:*

- *They have the same discriminant.*
- $a' = c \neq 0$.

- $b' \equiv -b \pmod{2c}$.

In this case we will also say that the form f is left adjacent to the form f'.

We define the *adjacency matrix* N_δ as

$$N_\delta := TS^\delta = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}.$$

If $f = (a, b, c)$, then $f|_{N_\delta} = (c, -b + 2c\delta, c\delta^2 - b\delta + a)$. The reason for its name is the following result:

Proposition 2.5. *Adjacent forms are equivalent by means of adjacency matrices.*

Proof. We do it just for the right adjacency. Suppose $f' = (a', b', c')$ is right adjacent to the form $f = (a, b, c)$. We define $\delta := \frac{b+b'}{2c}$. Note that it is an integer due to $b' \equiv -b \pmod{2c}$. The matrix N_δ makes $f|_{N_\delta} = f'$, for

$$\begin{pmatrix} 0 & 1 \\ -1 & \frac{b+b'}{2c} \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \frac{b+b'}{2c} \end{pmatrix} = \begin{pmatrix} c & \frac{b'}{2} \\ \frac{b'}{2} & a - \frac{b+b'}{2c}b + (\frac{b+b'}{2c})^2 c \end{pmatrix},$$

and since $c = a'$ and $b^2 - 4ac = b'^2 - 4a'c'$, the result follows immediately.

□

Definition 2.6. *We shall call a form* (a, b, c) ambiguous *if a divides b.*

These forms are interesting for they are improperly equivalent to themselves. Indeed, in general $(a, b, c), (c, b, a)$ are improperly equivalent, but (a, b, c) and (c, b, a) are also adjacent since $a = a, b + b \equiv 0 \pmod{2a}$, so we can compose this two transformations to arrive to the improperly equivalence of (a, b, c) and itself.

It remains just two kind of equivalences we would like to name. As we said before, the group $PSL(2, \mathbb{Z})$ acts on the right on the set of forms of discriminant D. Therefore, given a form f we can consider its stabilizer subgroup, i.e. the transformations $M \in PSL(2, \mathbb{Z})$ such that $f|_M = f$. Those transformations will be called *automorphs of f* and the stabilizer group of f as $Aut(f)$.

Similarly, we define an *antimorph* of a form (a, b, c) as a transformation M such that $f|_M = (-a, b, -c)$. Note that antimorphs do not form a group.

2.3 Principal root

Given a real number $x \geq 0$, when writing $\sqrt{x}$ we will be referring only to the nonnegative square root. On the other hand, if $x < 0$, when writing $\sqrt{x}$ we will be referring only to the square root whose imaginary part is positive.

Definition 2.7. The principal root *of a form* (a, b, c) *such that* $a \neq 0$ *is the complex number*

$$\omega = \frac{-b + \sqrt{D}}{2a}.$$

The principal root has great importance when studying a form, for actually quadratic extensions and binary forms are nearly the same thing, as the following proposition suggests:

Proposition 2.8. *Given* D *not a square, two forms with discriminant* D *and the same principal root are identical.*

Proof. Suppose the mentioned forms are $f = (a, b, c)$ and $f' = (a', b', c')$. We have

$$\frac{-b + \sqrt{D}}{2a} = \frac{-b' + \sqrt{D}}{2a'}.$$

Multiplying both sides by $2aa'$ and equaling the integer and the $\sqrt{D}$ terms, we get the two equations

$$a'b = b'a; \quad a' = a,$$

so $b = b'$. Using the equality of discriminant we arrive to $c' = c$.

□

This similarity can be taken further, and actually $Cl(D)$ is isomorphic to some class group of quadratic number fields. However we will not use that approach, so last result suffices for us. One of the nicest virtues of the principal root is that it is a very precise witness of the transformations acting on a form:

Proposition 2.9. *If the forms* f, f' *are properly equivalent via the transformation* $M := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, *i.e. if* $f|_M = f'$, *and their principal roots are* ω *and* ω' *respectively, then they satisfy*

$$\omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta}.$$

Conversely, if the principal roots of f *and* f' *satisfy the mentioned equation and* $\alpha\delta - \beta\gamma = 1$, *then the forms* f *and* f' *are properly equivalent via* M.

Proof. Let the forms be $f = (a, b, c)$ and $f' = (a', b', c')$. It is easy to check that the proposed equation is equivalent to

$$\omega' = \frac{\delta\omega - \beta}{-\gamma\omega + \alpha}.$$

The rest can be done by simple calculation. We write

$$\frac{\delta\omega - \beta}{-\gamma\omega + \alpha} = \frac{\delta\frac{-b+\sqrt{D}}{2a} - \beta}{-\gamma\frac{-b+\sqrt{D}}{2a} + \alpha} = \frac{-\delta b - 2a\beta + \delta\sqrt{D}}{\gamma b + 2a\alpha - \gamma\sqrt{D}}.$$

After multiplying the denominator and the numerator by $\gamma b + 2a\alpha + \gamma\sqrt{D}$, we simplify the resultant fraction, where the definition of the determinant is used. Comparing this to

$$\frac{-b' + \sqrt{D}}{2a'},$$

where the equivalence equations 2.1 let us substitute a' and b', we see they are identical.

Last process can be followed inversely, hence the reciprocal is also proven.

□

2.4 Representation of numbers

We say a form $f(x, y)$ represents an integer m if there exist integers x_0, y_0 so that $f(x_0, y_0) = m$. If $\gcd(x_0, y_0) = 1$ we will say such a representation is *primitive*.

The original problems related to binary forms were all related to representation of numbers, so it is not surprising that most of the properties we have stated have their "representational" aspect.

We are considering primitive forms. A natural question is whether the primitiveness is maintained upon equivalence or not. Indeed it is.

Proposition 2.10. *If $f = (a, b, c)$ and $f' = (a', b', c')$ are equivalent, then* $\gcd(a, b, c) = \gcd(a', b', c')$.

Proof. If $f|_M = f'$, where M is the usual transformation, it follows from the equivalence equations 2.1 of M and M^{-1}. For example we have

$$\begin{aligned} a\alpha^2 + b\alpha\gamma + c\gamma^2 &= a' \\ b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta) &= b' \\ a\beta^2 + b\beta\delta + c\delta^2 &= c' \end{aligned} \tag{2.2}$$

then it is obvious that any integer dividing all a, b, c must also divide a', b' and c'. We act analogously with M^{-1} and we are done.

□

The reason why we only considered primitive forms in some way lies on the representation problem, for forcing forms to satisfy this condition avoids "impure" representations.

The notion of equivalence is nearly identical to consider the whole set of numbers primitively represented by a form. For the sake of briefness, let's define $Rep(f) = \{f(x, y) \mid \gcd(x, y) = 1\}$. We have the following result:

Proposition 2.11. *If f and f' are equivalent, then $Rep(f) = Rep(f')$.*

Proof. Suppose $f = (a, b, c)$, $f' = (a', b', c')$ and $f|_M = f'$ via the usual transformation satisfying $\alpha\delta - \beta\gamma = 1$.

It is enough to prove that $Rep(f') \subset Rep(f)$, for using M^{-1} we would get the opposite inclusion. We have $f(\alpha x + \gamma y, \beta x + \delta y) = f'(x, y)$. So if $f'(p, q) = R$, then we have $f(\alpha p + \gamma q, \beta p + \delta q) = R$. Since $\alpha\delta - \beta\gamma = 1$, we deduce $1 = \gcd(p, q) = \gcd(\alpha p + \gamma q, \beta p + \delta q)$, which finishes the proof.

□

Actually last demonstration also works for improper equivalence. A particular consequence of this fact that we could have guessed just by looking at the equivalence equations 2.1 is that if $f = (a, b, c)$ and $f' = (a', b', c')$ are equivalent then f represents a' and c' and f' represents a and c.

The reciprocal also holds: two forms representing the same integers must be equivalent, although we will not prove it in order to avoid an aside on algebraic geometry.

Since $Rep(f)$ has such a great importance, it is natural to classify binary forms attending to differences in the represented sets. We already know something about this: when studying binary forms considering them as polynomials in $\mathbb{R}$, the Spectral Theorem establishes that there exists an orthogonal basis such that the matrix A_f becomes diagonal, being the coefficients of the diagonal its eigenvalues.

Let those eigenvalues be λ_1 and λ_2. We make the following distinctions:

- If $\lambda_1 > 0$ and $\lambda_2 > 0$, then f takes only positive values and f is positive definite. Analogously, if both eigenvalues are negative then f is negative definite. In this case $\det A_f > 0$.

- If $\lambda_1 \lambda_2 < 0$, we say the form is indefinite. Then f takes positive and negative values, and it may become zero at some point. In this case $\det A_f < 0$.

- If $\lambda_1 > 0$ and $\lambda_2 = 0$, then in the orthogonal basis f has the form $f(x, y) = \lambda_1^2 x^2$ (or its associate, but it has not importance). Then f takes nonnegative values, but also zero. We proceed similarly if $\lambda_1 < 0$ and $\lambda_2 = 0$. This forms are called (positive or negative) semidefinite. In this case $\det A_f = 0$.

This is what we would normally say in $\mathbb{R}$. However, let's go back to $\mathbb{Z}$, where this classification changes a bit. In order to not forget the tools we are provided with in this work, we suppose $f(x, y) = m$, where $x, y, m \in \mathbb{Z}$. We multiply this equation by $4a$ and complete the square to obtain

$$4am = (2ax + by)^2 - Dy^2. \tag{2.3}$$

The right hand side changes depending on the distinction stated above, taking into account $D = -4 \det A_f$. More concretely:

- If $D < 0$, we stated $Rep(f)$ is positive or negative and $\operatorname{sgn} a = \operatorname{sgn} m$. Indeed, the right side $(2ax + by)^2 - Dy^2$ is always greater than zero. This one is the *definite case*.

- If D is positive but not a square, then $Rep(f)$ contains positive and negative values, but it does not contain the zero, as it can easily be checked in equation 2.10.1. We call this the *indefinite case*.

- If $D = h^2$, with h a nonnegative integer, then the right side can be written as $(2ax + by + hy)(2ax + by - hy)$, and it does contain the zero, hence so does $Rep(f)$. We call this the *square case*, which is a *degenerated case*.

- If $D = 0$ then the right hand side is a perfect square and $Rep(f)$ is either nonnegative or non-positive, and in both cases it contains zero. For us, this will be a *degenerated case*.

All these cases will be carefully studied.

Chapter 3

Automorphs and Pell's equation

From now on, we will refer to the equation $x^2 - Dy^2 = \pm 4$ as Pell's equation, the equation with only the plus sign as positive Pell's equation and the equation with only the minus sign as negative Pell's equation.

Definition 3.1. *The set $Pell(D)$ is the set of all solutions (x, y) to positive Pell's equation such that $x \geq 0$. The solution $(2, 0) \in Pell(D)$ is called the trivial solution.*

Similarly, the set $nPell(D)$ is the set of all solutions (x, y) to negative Pell's equation such that $x \geq 0$.

There is a small detail we did not include in the definition in order to make it clearer. It is that, in $Pell(D)$, in case $x = 0$ we will just include the solution with positive y. This convention allows us to state the results of this chapter in a much nicer way.

We have defined these sets but we do not know yet whether they are empty or not. For example, let's take a look at the positive one:

- If $D = 0$, then $Pell(D) = \{(2, y)\}_{y \in \mathbb{Z}}$.
- If $D < 0$ then the positive Pell's equation has non-trivial solutions only if $D = -1$, $D = -3$ or $D = -4$. If $D = -1$ the only non-trivial solution is $(0, 2)$. For $D = -3$, $(1, \pm 1)$. When $D = -4$, the non-trivial solutions are $(0, 1)$.

- If $D = h^2 > 0$, equation $(x + hy)(x - hy) = 4$ has just the trivial solution.

On the other hand, $nPell(D) = \{\emptyset\}$ for all $D \leq 0$, and if $D = h^2 > 0$ the only non-empty sets are $nPell(1) = \{(0, \pm 2)\}$ and $nPell(4) = \{(0, \pm 1)\}$.

The rest of cases, i.e. when D is positive and not a square is much more interesting. We have the following result, which is known enough to not be proven (it can be found in [2], for example):

Proposition 3.2. *If D is a positive discriminant and the set $Pell(D)$ contains any non-trivial solution, then the non-trivial solution $(X, Y) \in Pell(D)$ with mimimum X satisfies that for every $(x, y) \in Pell(D)$ there exists $n \in \mathbb{Z}$ such that*

$$\frac{x + y\sqrt{D}}{2} = \frac{(X + Y\sqrt{D})^n}{2^n},$$

and conversely every pair (x, y) satisfying last equation belongs to $Pell(D)$.

The existence of solutions of Pell's equation is related to the structure of morphisms between forms of a given discriminant, which is the reason why we are talking about this equation. We have the following result:

Proposition 3.3. *Suppose we are given a discriminant D and any form f with that discriminant.There is a one-to-one correspondence between $Aut(f)$ and $Pell(D)$.*

Proof. First we assume $f = (a, b, c)$ and $f|_M = f$, where $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, not $\pm$Id. We can suppose $\alpha + \delta \geq 0$. Then, if ω is the principal root of f we have

$$\omega = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}.$$

This equation can be rewritten as

$$\gamma\omega^2 + \omega(\delta - \alpha) - \beta = 0.$$

Since the form (a, b, c), as almost all forms we consider in this work, is assumed to be primitive and we already have $a\omega^2 + b\omega + c = 0$, we must have

$$\gamma = ka \quad , \quad \delta - \alpha = kb \quad and \quad \beta = -kc$$

for k a nonzero integer. So using the definition of the discriminant we get

$$(\delta - \alpha)^2 + 4\gamma\beta = Dk^2,$$

which can be simplified using $\alpha\delta - \beta\gamma = 1$ as

$$(\alpha + \delta)^2 - Dk^2 = 4.$$

This is a trivial solution only if $k = 0$.

Now we assume we are given a non trivial solution $(x, y) \in Pell(D)$ of the equation. Then the transformation

$$\begin{pmatrix} \frac{x-by}{2} & -cy \\ ay & \frac{x+by}{2} \end{pmatrix}$$

is an automorph of the form (a, b, c). Note the coefficients are integers since $b \equiv D \pmod 2$ and $x^2 - Dy^2 = 4$.

In can be easily seen that each of these two correspondences are inverse of the other one, hence we have described a one-to-one correspondence.

□

Let's write explicitly the bijection supposing $a \neq 0$:

$$\begin{aligned} \phi\colon Aut(f) &\to Pell(D) \\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} &\mapsto (\alpha + \delta, \frac{\gamma}{a}) \end{aligned}$$

where we supposed $\alpha + \delta \geq 0$. Its inverse is

$$\begin{aligned} \phi^{-1}\colon Pell(D) &\to Aut(f) \\ (x, y) &\mapsto \begin{pmatrix} \frac{x-by}{2} & -cy \\ ay & \frac{x+by}{2} \end{pmatrix} \end{aligned}$$

where we supposed $x \geq 0$.

The fact that we have a bijection between two groups suggests that we could try to be more ambitious and prove it is an isomorphism. Regarding the existence of solutions to the positive Pell's equation when D is positive and not a square, later we will prove that there exists always an automorphism of a form f with discriminant D by means of more adequate mathematical objects.

Similarly, the negative Pell's equation is related to another kind of transformation:

Proposition 3.4. *Suppose we are given a discriminant D and any form f with that discriminant. There is a one-to-one correspondence between antimorphs of forms f and $nPell(D)$.*

Proof. We act analogously as we did with the automorphs. Suppose there exists an antimorph $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ of the form (a, b, c), where we suppose $\alpha - \delta \geq 0$. If the principal root of (a, b, c) is ω, then the principal root of $(-a, b, -c)$ is $-\omega$ and we have the equation

$$\omega = \frac{\alpha(-\omega) + \beta}{\gamma(-\omega) + \delta},$$

which becomes

$$\gamma\omega^2 - (\alpha + \delta)\omega + \beta = 0.$$

Since $a\omega^2 + b\omega + c = 0$ and using the primitiveness of (a, b, c), we deduce $\gamma = ka, \alpha + \delta = -kb$ and $\beta = kc$. This gives

$$(\alpha + \delta)^2 - 4\gamma\beta = k^2 D,$$

where D is the determinant of the form (a, b, c). It becomes

$$(\alpha - \delta)^2 - Dk^2 = -4,$$

as desired.

Now we assume we are given a solution (x, y) of the equation $x^2 - Dy^2 = -4$. We consider the transformation

$$\begin{pmatrix} \frac{x-by}{2} & cy \\ ay & \frac{-x-by}{2} \end{pmatrix}.$$

It is straightforward to show that it is a transformation of (a, b, c) into $(-a, b, -c)$.

Since these two correspondences are inverse of each other, we have described a one-to-one correspondence.

□

Unfortunately, the existence of solutions to negative Pell's equation depends on D and it is not as easy to decide which ones have solution and which do not.

Chapter 4

Definite forms

Forms with negative discriminant are those which are positive definite or negative definite. If the form (a, b, c) has discriminant $D < 0$ then a, c are both nonzero since the opposite would imply $-D = b^2 > 0$. For the same reason, both a, c are positive or negative. We will implicitly assume that all the forms in this chapter have negative discriminant.

Given a negative discriminant D, let's consider the application

$$\phi : (a, b, c) \mapsto (-a, -b, -c),$$

which bijectively maps the set of positive definite forms into the set of negative definite forms. We remark that there are no possible equivalences between these two sets, for no positive definite form represents the same integers as any negative definite form (actually, they do not both represent any integer at all). This means that studying only the positive definite forms will make us understand also the negative ones.

Hence, from now on, we will just consider the case where a, c are positive, i.e. the positive definite one.

Definition 4.1. *We shall call a form $f = (a, b, c)$* reduced *if is satisfies $|b| \leq a \leq c$ and, in case $a = |b|$ or $a = c$, if it also satisfies $b \geq 0$.*

The usefulness of this distinction will be explained soon. But first we need some results.

Proposition 4.2. *If $f = (a, b, c)$ is reduced and has discriminant $D < 0$, then $|b| \leq \sqrt{-D/3}$.*

Proof. Using the definitions, we have

$$4b^2 \leq 4ac \leq b^2 - D,$$

hence we deduce $3b^2 \leq -D$, as desired.

□

Proposition 4.3. *Given a discriminant $D < 0$, there is a finite number of reduced forms with such discriminant.*

Proof. Attending to last proposition, fixed D, the number of possible b is finite. Since $4ac = -D + b^2$, given b, the number of possible a, c is finite, so we are done.

□

Proposition 4.4. *Every class in $Cl(D)$ contains at least one reduced form.*

Proof. Suppose we are given a form $F_0 = (a_0, b_0, a_1)$ with negative discriminant D. We are going to find a reduced form (A, B, C) equivalent to the given one.

In case F_0 satisfies all the desired conditions, we are done. Otherwise, we act as follows.

We can consider b_1, the minimum absolute residue of $-b_0$ modulo $2a_1$. In other words, $b_1 \equiv -b_0 \pmod{2a_1}$ and $|b_1| \leq |a_1|$.

Let's also consider $a_2 := \frac{(b_1)^2 - D}{4a_1} > 0$, which is obviously an integer attending to the definition of b_1 and D.

So now let's look at the form $F_1 = (a_1, b_1, a_2)$. If $a_2 < a_1$, we repeat the process similarly. Sooner or later we will get $F_m = (a_m, b_m, a_{m+1})$ so that $a_{m+1} \geq a_m$ since otherwise we would get an infinite decreasing succession of integers $(a_m), m \in \mathbb{N}$, which is absurd. We claim that the form F_m satisfies all the desired properties.

First of all, in the succession $F_0, \cdots, F_m$ every form is adjacent to the next one, hence every form is equivalent to the next one, therefore F_0 is properly equivalent to F_m.

Moreover, $a_{m+1} \geq a_m$ from the way in which we constructed F_m.

Since b_m is the minimum absolute residual of $-b_{m-1}$ modulus $2a_m$, it satisfies $|b_m| \leq a_m$.

Hence we choose $(A, B, C) = (a_m, b_m, a_{m+1})$ and we are done.

□

Proposition 4.5. *Every class in $Cl(D)$ contains one unique reduced form.*

Proof. Suppose we are given the equivalent reduced forms $f = (a, b, c)$, $f' = (a', b', c')$. Without loss of generality, $a' \leq a$. Let's say the form f equivalently transforms into f' using the change of variable $M := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. From the equivalence equations 2.1:

1. $a\alpha^2 + b\alpha\gamma + c\gamma^2 = a'$
2. $a\alpha\beta + \frac{b}{2}(\alpha\delta + \beta\gamma) + c\gamma\delta = \frac{b'}{2}$
3. $\alpha\delta - \beta\gamma = 1$

From (1) we get $aa' = (a\alpha + \frac{b}{2}\gamma)^2 - \frac{D\gamma^2}{4}$, so $aa' > 0$ (remember they cannot be zero). Moreover, since $\operatorname{sgn}(a) = \operatorname{sgn}(c)$ and $\operatorname{sgn}(a') = \operatorname{sgn}(c')$, then a, a', c, c' they all must have the same sign. From the definition of reduced form, $aa' \leq \frac{-D}{3}$, therefore $\frac{-D\gamma^2}{4} = aa' - (a\alpha + \frac{b}{2}\gamma)^2 \leq \frac{-D}{3}$. Thus $|\gamma| \leq 1$.

In case $\gamma = 0$, from (3) we deduce that $\alpha = \delta = 1$ or $\alpha = \delta = -1$. They lead us to $a = a'$, $b - b' = \pm 2\beta a$. But from the definition and assumptions we have $|b| \leq |a|$ and $|b'| \leq |a'| \leq |a|$, hence the only two possibilities are

- $b = b'$, which implies $c' = \frac{b'^2 - D}{4a'} = \frac{b^2 - D}{4a} = c$, so all in all the forms are the same one, against the hypothesis.

- $b = -b' = \pm a$, which implies $c = c'$ and $(a', b', c') = (a, -b, c)$, i.e. they are opposed. Plus, they are ambiguous since $b = \pm a$. Attending to the definition of reduced form, both b and b' should be nonnegative, but this implies $a = b = 0$, which is an absurd, for the discriminant would be zero.

In case $\gamma = \pm 1$, using the inequalities with (1), we get $\alpha = 0$ or $\alpha = \pm 1$.

If $\alpha = 0$, from (1) we get $a' = c$, and since $|a'| \leq |a| \leq |c|$ and they share sign, $a = a' = c$. From (3) and (2) we get $b + b' = \pm\delta a$. Similarly as in the previous situation, this implies

- $b = b'$, hence c = c', and the forms f, f' would be identical, against the hypothesis..

- $b = -b'$, which implies $c = c'$, and the two forms would be opposed. The definition of reduced form leads us to $b = b' = 0$, hence the forms F, F' would be identical, again a contradiction.

If $\alpha = \pm 1$, from (1) we get $\pm b = a + c - a'$. We have $|a'| \leq |a| \leq |c|$ and $\text{sgn}(a) = \text{sgn}(c) = \text{sgn}(a')$, so $|b| \geq |c| \geq |a|$. Using the inequalities from the definition of reduced form, $\pm b = a = c$, so moreover $\pm b = a'$. From (2) and (3), we can deduce

$$b - b' = 2a(\alpha\beta + \delta\gamma) + 2b\beta\gamma = 2a(\alpha\beta + \delta\gamma \pm \beta\gamma),$$

so similarly as in the two previous situations, this implies

- $b = b'$, and the two given forms would be identical, against the hypothesis.

- $b = -b'$, and the two forms would be opposed. Moreover, they are ambiguous since $a = \pm b$. As before, this is not possible.

We have checked all possibilities, therefore we are done.

□

During last demonstration, the definition of reduced form proved to be useful, for it assures the uniqueness of reduced forms in their classes. The condition $b \geq 0$ for the cases $a = |b|$ or $a = c$ is necessary, for we have the following equivalences:

- $(a, a, c) \sim (a, -a, c)$. It can be obtained as follows: in general we have $(a, a, c) \sim (c, -a, a)$, so we can use that $(c, -a, a)$ and $(a, -a, c)$ are adjacent to deduce the desired equivalence.

- $(a, b, a) \sim (a, -b, a)$ since they are adjacent.

Actually the last argument could be used to determine which determinants have reduced forms with non-trivial automorphs and which ones have not. Easily we would get the only possible options are $(1, 1, 1)$, so $D = -3$, for the first case; and $(1, 0, 1)$, so $D = -4$, for the second. If we recall what we explained about the existent relation between automorphs and positive Pell's equation we would not need to consider the previous proof, for we already enumerated the simple cases of $Pell(D)$ and from the bijection we established we can express their respective automorphs easily.

For example, for $D = -3$, for the reduced form $f = (1, 1, 1)$, we have $Aut(f) =< TS >= \{\text{Id}, TS, (TS)^2\}$.

When $D = -4$, for $f = (1, 0, 1)$, we have $Aut(f) =< T >= \{\mathrm{Id}, T\}$.

Now it is a good point to stop to analyze what we have done. Given the discriminant $D < 0$, there is a finite number of reduced forms (a, b, c) with such discriminant. Plus, every form is properly equivalent to one reduced form.
Therefore $Cl(D)$ is finite and for every class in $Cl(D)$ we can choose a representative which is its unique reduced form. Achieving this was the aim of this chapter.

Chapter 5

Indefinite forms

We will consider now forms with determinant $D > 0$, not a square, which are called indefinite. The non center terms of the form cannot be zero. We will implicitly assume that all forms in this chapter have a discriminant of this kind.

Definition 5.1. *A form (a, b, c) is called* reduced *if*

$$0 < b < \sqrt{D}$$

$$\sqrt{D} - b < 2|a| < \sqrt{D} + b.$$

Lemma 5.2. *Let (a, b, c) be a reduced indefinite form. The following inequalities hold:*

1. $ac < 0$
2. $\sqrt{D} - b < 2|c| < \sqrt{D} + b$
3. $|a| < \sqrt{D} \quad ; \quad |c| < \sqrt{D}$
4. $\sqrt{D} - 2|a| < b \quad ; \quad \sqrt{D} - 2|c| < b$

Proof. Them all easily follow using the definitions:

1. From $0 < b < \sqrt{D}$ we get $ac = b^2 - D < 0$, hence a and c have opposite sign.
2. We have $(\sqrt{D} - b)(\sqrt{D} + b) = 2|a|2|c|$. Supposing $2|c|$ does not belong to the mentioned interval, we easily deduce that $2|a|$ does not belong to this interval either, against the hypothesis.

3. Since $2|a| < \sqrt{D} + b$ and $0 < b < \sqrt{D}$, we have $2|a| < 2\sqrt{D}$. Analogously with c.
4. We have $\sqrt{D} - b < 2|a|$, so $\sqrt{D} - 2|a| < b$. Analogously with c.

□

Attending to the second equality, if (a, b, c) is a reduced form then also its associated form (c, b, a) is reduced.

Another consequence of this lemma is the following one:

Proposition 5.3. *Given $D > 0$, not a square, the number of reduced forms with that discriminant is finite.*

Proof. The number of possible a, b, c is bounded, hence so it is the number of possible forms (a, b, c).

□

Now, we would like to arrange these forms the same way we did with the definite ones. To begin with, we have the following result:

Proposition 5.4. *Every class in $Cl(D)$ contains at least one reduced form.*

Proof. Assume we are given a non reduced indefinite form $f_1 = (a_1, b_1, c_1)$ with discriminant D. We aim to find a reduced form $F = (A, B, C)$ equivalent to the given one. We are going to create an algorithm as we did with the definite ones.

First we choose the unique δ_1 so that

$$\sqrt{D} - 2|c_1| < -b_1 + 2c_1\delta_1 < \sqrt{D},$$

which obviously exists. We apply the transformation $N_{\delta_1} = \begin{pmatrix} 0 & 1 \\ -1 & \delta_1 \end{pmatrix}$ to f_1, which converts it into one of its right adjacent forms

$$f_2 : (c_1, -b_1 + 2c_1\delta, a_1 - b_1\delta + c_1\delta^2),$$

and they satisfy $f_1 \sim f_2$.

If f_2 is reduced, we are done.

Otherwise we start this process again naming $f_2 := (a_2, b_2, c_2)$ and so on until for some integer i we have $|c_{i+1}| \geq |a_{i+1}| = |c_i|$, which has to happen by infinite descent. Then we will have a form $F = (A, B, C) := (a_i, b_i, c_i)$ so that $|A| \leq |C|$, $\sqrt{D} - 2|A| < B < \sqrt{D}$, and $f_1 \sim F$ due to the transitivity of the relation of equivalence '$\sim$'.

So we already have $\sqrt{D} - B < 2|A|$. Using $|\sqrt{D} - B||\sqrt{D} + B| = 4|A||C|$, we deduce that we must also have $|\sqrt{D} + B| > 2|C|$. All in all

$$|\sqrt{D} + B| > 2|C| > 2|A| > \sqrt{D} - B.$$

Since $|\sqrt{D} + B| > \sqrt{D} - B$, B must be positive. Hence (A, B, C) is reduced, so we are done.

□

We cannot state the uniqueness of these reduced forms in each class of $Cl(D)$. Actually, they form cycles of equivalent forms where every form is "connected" to its two only adjacent forms.

Proposition 5.5. *Every reduced form has exactly one right adjacent reduced form and exactly one left adjacent reduced form.*

Proof. Suppose we are given a reduced form (a, b, c) with discriminant D. We will show this proposition for the right adjacency, the left one follows analogously. To do so, we search for one form (a', b', c'), reduced and also right adjacent to the given one. We must prove there exists exactly one form satisfying this.

Is is *necessary* that the form (a', b', c') satisfies the adjacency equations $a' = c$, $b' \equiv -b \pmod{2|a'|}$ and the equality of determinant, hence once we will determine b', the form will be determined.

It is also *necessary* that the form (a', b', c') satisfies the reduced inequalities, in particular the inequality $\sqrt{D} - 2|a'| < b' < \sqrt{D}$.

Attending to this two necessary conditions, the term b', hence the form (a', b', c'), is uniquely determined. It is left to prove that this form is actually reduced. In other words, we have to prove

$$0 < b' \quad ; \quad 2|a'| < \sqrt{D} + b'.$$

Let's set the following definitions:

$$p := \sqrt{D} + b - 2|a| \; ; \; q := 2|a| - (\sqrt{D} - b) \; ; \; r := \sqrt{D} - b$$

$$q' := 2|a'| - (\sqrt{D} - b') \; ; \; r' := \sqrt{D} - b'$$

Since (a, b, c) is a reduced form, we deduce that p, q, r are positive. From the construction of b', also q', r' are positive.

Now let's write $b' = -b + 2|a|m$, m an integer. Since

$$0 < p + q' = b + b' = 2|a|m,$$

it must be $m - 1 \geq 0$. Moreover,

$$2b' = r + q' + 2|a|(m - 1) > 0,$$

so $b' > 0$, as desired. We also have

$$0 < r + 2|a'|(m - 1) = \sqrt{D} + b' - 2|a'|,$$

so $2|a'| < \sqrt{D} + b'$, which finishes the proof.

□

Using this proposition, we can partition the set of reduced forms of a given discriminant into cycles. To do so, we choose any reduced form f_1 and start a cycle moving forward to the next right adjacent form, which gives us the forms $f_2, f_3, \cdots$. Since the reduced forms of a given discriminant are finite, sooner or later we will return to a form we have already passed by, therefore we can define m as the smallest natural so that there exists $n \in N$, $n < m$, satisfying $f_n = f_m$. We claim that $n = 1$. Indeed, if we had $n > 1$, we could consider f_m and f_n and move to their left adjacent forms, i.e. f_{m-1} and f_{n-1}. Since the adjacent reduced forms are unique, they satisfy $f_{n-1} = f_{m-1}$, which contradicts the definition of m.

So, the cycle which started in f_1 eventually returns to f_1 without having repeated any other form before. If there are no reduced forms left, we finish the process. Otherwise, we choose a new reduced form not belonging to any of the considered cycles and repeat the process, until we completely finish.

Since adjacent forms are equivalent, these cycles are composed of equivalent forms. So a natural question is whether the reciprocal also holds. Indeed it does, although we cannot demonstrate this theorem yet since we will need further theory to prove it, regarding the existent relation between continued fractions and forms.

5.1 Behavior of the cycles

The number of forms in any cycle is called the *period* of the cycle.

Proposition 5.6. *The period of any cycle is even.*

Proof. As we proved, in any reduced indefinite form (a, b, c) of determinant D, a, c are non zero and have opposite sign. Starting from a random form, we move towards the next right adjacent form, whose left term has opposite sign to the left term of the previous form. Since every step the sign changes and we must return to the original form, i.e. to the same sign, the parity of the number of steps is even, and so it is the period of the cycle.

□

Now let's assume the associated forms $f = (a, b, c)$ and $f' = (c, b, a)$ are in different cycles. Then moving towards the right adjacent form of f we will get the associated form of that one we get moving towards the left adjacent form of f', and so on if we continue the process. Thus, we call these cycles *associated*.

Proposition 5.7. *Given a cycle, if it contains one ambiguous form, then it contains exactly two and the given cycle is its own associate. Conversely, if the given cycle is its own associate, then it contains exactly two ambiguous forms.*

Proof. Suppose the cycle contains the ambiguous form (a, ak, c). Its associate (c, ak, a) is also its right adjacent form since $2ak \equiv 0 \pmod{2a}$. Thus, cycling forward from (c, ak, a) and backwards from (a, ak, c), we get successively pairs of associate forms, and since the cycle is finite and its period even, we finish the process when we arrive to the last pair of forms, which are adjacent and associated. Therefore, the form we got cycling from (c, ak, a) is the other ambiguous form (note it could be the form (c, ak, a) itself in case there are no more forms). Attending to the way the pairs of associated forms were distributed, the two ambiguous forms we have mentioned are the only two possible. From the process we have just followed, we also deduce that the given cycle is its own associate.

Now we assume the given cycle is its own associate. We will follow a similar strategy. A form cannot be its own associate, so we choose two different associated forms f, f' and cycle forward from f and backwards from f' through pairs of associated forms. In other words, we are moving just in one arc of the cycle. Note that, from the change of sign criteria, this arc has an even number of forms. Since this arc is finite, eventually we come up with two adjacent associated forms $(a', b, a) \sim (a, b, a')$. From the adjacency, $b + b \equiv 0 \pmod{2a}$, hence (a, b, a') is ambiguous. Using the other arc of the cycle, we could get a different ambiguous form, so we have

two of them. The cycle cannot contain more since following this process we checked all the forms in it. This finishes the proof.

□

The most relevant associated cycle is *the principal cycle*. It cannot be defined as the one containing the principal form I_D, for it is not reduced, so we define it as the one containing the *principal reduced form* of discriminant D, defined as $I_p := (1, b, -\frac{-D-b^2}{4})$ where b has the following value:

$$b := \left\lceil \sqrt{D} \right\rceil - 2 \text{ if } \left\lceil \sqrt{D} \right\rceil \text{ and } D \text{ have the same parity}$$

$$b := \left\lceil \sqrt{D} \right\rceil - 1 \text{ if } \left\lceil \sqrt{D} \right\rceil \text{ and } D \text{ have opposite parity}$$

With this definition, the principal reduced form is actually reduced. Its principal root is $\omega_p := \frac{-b+\sqrt{D}}{2}$. The principal reduced form $I_p = (1, b, c)$ is equivalent to $I_D = (1, b', c')$, for $1 = 1$ and $b \equiv b' \pmod 2$ since they share discriminant. Actually, any form whose left term is 1 having discriminant D must be equivalent to I_p.

Since the form I_p is ambiguous, last proposition implies that the principal cycle contains one more ambiguous form and it is its own associate. This fact means that just half of the cycle has "new" information.

5.2 Cycles and continued fractions

A key fact in the theory of forms is that developing the principal root of a form as a continued fraction and moving forward in the cycle that contains that form are *essentially* the same thing.

To prove so, we consider any reduced form (a, b, a') and its right adjacent one in the cycle, (a', b', a''). During the next argument, it will be relevant that a and a'' have the same sign, which is opposite to the sign of a'. We set $\delta := -\frac{b+b'}{2a'}$ and, as we proved, the two forms are properly equivalent by means of the transformation $\begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}$. Therefore, if ω and ω' are the two principal roots of the forms considered, we have

$$\omega = \frac{1}{\delta - \omega'}.$$

Since $\omega = \frac{-b+\sqrt{D}}{2a}$, attending to the definition of reduced form, if a is positive then ω is a proper fraction, δ is positive and $\omega' = \frac{-b'+\sqrt{D}}{2a'}$ is negative.

Therefore, we get

$$\omega = |\omega| = \frac{1}{\delta - \omega'} = \frac{1}{|\delta| + |\omega'|}.$$

Similarly, if a is negative we arrive again to the equation $|\omega| = \frac{1}{|\delta|+|\omega'|}$.

Now, if we repeat the process, assuming the form (a', b', a'') becomes its right adjacent one via the transformation $\begin{pmatrix} 0 & 1 \\ -1 & \delta' \end{pmatrix}$, we would get

$$|\omega'| = \frac{1}{|\delta'| + |\omega''|}.$$

The pattern is clear: given a cycle of period $2m$, we set $f_1, \cdots, f_{2m}$ as the forms that compound the cycle. Assuming $\begin{pmatrix} 0 & 1 \\ -1 & \delta_k \end{pmatrix}$ is the transformation which converts f_k into f_{k+1}, and writing $d_k := |\delta_k|$ and also ω_k as the principal root of f_k, then the following scf expansion holds

$|\omega_1| = [0; *d_1, \cdots, *d_{2m}]$. Or more generally,

$|\omega_k| = [0; *d_k, \cdots, *d_{k+2m-1}]$, where $R > 2m$ implies , $w_R = w_{R-2m}$.

Since the sign of δ_k alternates each step, given the scf of ω_k we could deduce all the transformations in the cycle.

During the previous process we asked the form (a, b, a') to be reduced, but we could have tried to do something similar if we had started from any primitive form and then applied the reduction algorithm explained in proposition 5.4. In that case, we would not have been able to control the sign of the consecutive coefficients. We will supply this lack using proposition 1.7.

5.3 Applications of cycles

Since we have studied the properties of reduced indefinite forms, the stated parallelism between scf's and cycles must have some consequences.

For example, as we promised in the preamble, we can characterize a periodic scf as follows:

Proposition 5.8. *The scf of $\omega \in \mathbb{R}$ is periodic iff ω is an irrational root of a quadratic equation with integer coefficients.*

Proof. ($\Rightarrow$) Let $\omega = [a_0; \cdots, *a_I, \cdots, *a_{I+p-1}]$ and $X_I = [*a_I; \cdots, *a_{I+p-1}]$. If P'/Q' and P''/Q'' are the last two convergents of $[a_I; \cdots, a_{I+p-1}]$ then, since $X_I = [a_I; \cdots, a_{I+p-1}, X_I]$, using proposition 1.2 we deduce

$$X_I = \frac{P'X_I + P''}{Q'X_I + Q''},$$

therefore after manipulating this fraction we see X_I is a quadratic irrational. Now we have

$$\omega = [a_0; \cdots, a_{I-1}, X_I].$$

We could write

$$\omega = \frac{P_{I-1}X_I + P_{I-2}}{Q_{I-1}X_I + Q_{I-2}},$$

and using that quadratic real numbers (rationals included) form a field, we could deduce that ω is also a quadratic irrational. In case we do not want to use the fact that they form a field, we simply need the weaker result that given a rational r, if x is a quadratic irrational then xr and $x + r$ and $\frac{1}{x}$ are quadratic irrationals. Then we could consider $\omega = [a_0; \cdots, a_{I-1}, X_I]$ and isolating X_I in the right side we would get the desired result.

($\Leftarrow$) Let's suppose we have $a\omega^2 + b\omega + c = 0$, where a, b, c are coprime. We consider the form $f = (a, b, c)$, probably not reduced. It is possible that ω is the conjugate of the the principal root of f, but since we could consider the form $(-a, -b, -c)$ instead, we can suppose that ω is principal. There exists at least one reduced form $F = (A, B, C)$ so that $f \sim F$, where we can suppose $A > 0$ (otherwise, we consider its right adjacent form instead). Let $\Omega > 0$ be the principal root of F. Since these two forms are equivalent, we can get $\alpha\delta - \beta\gamma = 1$ satisfying

$$\omega = \frac{\alpha\Omega + \beta}{\gamma\Omega + \delta},$$

therefore we apply proposition 1.7 and get

$$\omega = [u; a_1, \cdots a_{2r}, v, \Omega].$$

We can assume $\Omega = [0; *d_1, \cdots, *d_{2m}]$. If $v + d_1$ is positive, we are done. In case it is negative, we apply the method of proposition 1.6 and, changing just a finite number of quotients, we make that continued fraction a scf. Since just a finite number of quotients were altered, and since the scf of Ω is periodic, eventually in the scf of ω we must arrive to a period, as we wanted to prove.

□

For the case when ω is pure periodic we can be much more precise:

Proposition 5.9. *The scf of a positive real number ω is pure periodic iff it is the principal root of a reduced form (a, b, c) with a positive.*

Proof. ($\Leftarrow$) It follows directly from the method described at the beginning of this chapter.

($\Rightarrow$) The following demonstration is based on the same strategy we will use to prove that equivalence implies sharing cycle, therefore we will not give as many details as we do in theorem 5.12, where more details are explained. Suppose ω has a pure periodic scf $[0; *a_1, \cdots, *a_p]$, where p is minimum. Since it is periodic, we know there exist unique coprime a, b, c so that

$$a\omega^2 + b\omega + c = 0,$$

where we can suppose ω is the principal root. We consider the form $f = (a, b, c)$ and repeat exactly the same process we used in the second part of last proposition: there exists a reduced form $F = (A, B, C)$ with $A > 0$ so that its principal root Ω is pure periodic and satisfies

$$\omega = [u; a_1, \cdots a_{2r}, v, \Omega].$$

We apply proposition 1.6 and, after altering a finite number of quotients, it becomes a scf as $\omega = [l_0; l_1, \cdots]$. Since an infinite scf is unique, from $[0; *a_1, \cdots, *a_p] = [l_0; l_1, \cdots]$ we can deduce that all quotients are identical. Since just a finite number of quotients where altered, the period of Ω must be a cyclical permutation of that of ω. Therefore if we move to the right adjacent form starting from F, after an even number of steps we will arrive to a form f' so that its principal root, also positive, has the same scf as f. Using proposition 10.6, this implies that f' and f are the same form, hence f is reduced, as desired.

□

So we have two distinct but related objects: cycles, which can be measured by using their period, and pure periodic simple continued fractions, which also have their period. There is still something we should clarify about them, for it could happen that the period the principal root ω is a divisor of the period of the cycle $2m$. Following the notation used before, we consider a form $f_1 = (a, b, c)$ and moving forward in the cycle of period $2m$ we get the coefficients $\delta_1, \delta_2 \cdots \delta_{2m}$. Also suppose f_1 has principal root ω_1 of period p. We already know p divides $2m$, but we want to improve this.

Proposition 5.10. *In last situation, there are just two options: $p = 2m$ or $p = m$. If $p = m$, then the form $(-a, b, -c)$ also belongs to the cycle and m is odd.*

Proof. We assume $\omega_{2m+1} = \omega_1$. In general, we have

$$|\omega_1| = [d_1; \cdots, d_p, \frac{1}{|\omega_{p+1}|}].$$

However, from the hypothesis we also have

$$|\omega_1| = [d_1; \cdots, d_p, \frac{1}{|\omega_1|}].$$

Isolating $|\omega_{p+1}|$ and $|\omega_1|$ in the right hand side, we get $|\omega_1| = |\omega_{p+1}|$. Two options arise:

1. $\omega_{p+1} = \omega_1$. Using proposition 10.6, this implies $f_1 = f_{p+1}$. Since the cycle has period $2m$ (and not smaller), the only possible option is $p = 2m$.

2. $\omega_{p+1} = -\omega_1$. Since $(-a, b, -c)$ is reduced, has determinant D and principal root $-\omega_1$, using proposition 10.6 it must be $f_{p+1} = (-a, b, -c)$. Suppose (a', b', c') is the right adjacent form of f_{p+1}, and (a_2, b_2, c_2) the right adjacent form of f_1.The process to build the right adjacent form explained in proposition 5.5 states that $a' = -c$, $b' \equiv -b \pmod{2|-c|}$, so we have $(a', b', c') = (-a_2, b_2, -c_2)$; $\delta_{p+1} = -\delta_1$, and repeating the process $\delta_{p+2} = -\delta_2 \cdots$

   Therefore the steps (moving to the right adjacent form) from f_1 until f_{p+1} and from f_{p+1} until f_1 are equal, so it must be $f_{p+1} = f_{m+1}$, hence $p = m$. Since $\delta_{m+1} = -\delta_1$ and the sign of δ_k alternates each step, m must be odd, which finishes the proof.

□

Now we suppose the form (a, b, c) is reduced. In that case, as we said, also $(-a, b, -c)$ is reduced, and their principal roots ω and ω' satisfy $\omega = -\omega'$, hence the scf of their absolute values coincide. The following proposition clearly states the reciprocal of the second item of last proposition.

Proposition 5.11. *If the reduced forms (a, b, c) and $(-a, b, -c)$ belong to the same cycle of period $2m$, the period of ω is m and m is odd.*

Proof. We will follow the notation used before. We write $f_1 := (a, b, c)$ and we move forward in the cycle and get the coefficients $\delta_1, \delta_2 \cdots$ We do the same starting from $\phi := (-a, b, -c)$ and get the coefficients $-\delta_1, -\delta_2 \cdots$, as we explained in last proposition. Therefore the steps (moving to the right adjacent form) from f_1 until ϕ and from ϕ until f_1 are equal, so it must be

$\phi = f_{m+1}$, and
$\delta_{m+1} = -\delta_1, \quad \delta_{m+2} = -\delta_2 \cdots \quad \delta_{2m} = -\delta_m$. All in all

$$d_{m+1} = d_1, \quad d_{m+2} = d_2 \cdots \quad d_{2m} = d_m,$$

which is one of the desired results.

The oddness of m follows from $\delta_{m+1} = -\delta_1$. Since every step the sign of δ_k alternates, if after m steps the sign is opposite then m must be odd, which finishes the proof.

□

The previous proof revealed that all the forms of a cycle of this kind may be arranged in pairs $(a, b, c), (-a, b, -c)$, where the second one lies m steps away from the first one. When considering the antimorphs, we proved that given a positive determinant D, the existence of this kind of equivalences depends on the negative Pell's equation. We will return to this point later.

Last results, carefully studied, help us to predict the possible period of the scf of all numbers of the type $\frac{-b+\sqrt{D}}{2a}$, where $a \neq 0$ and b are integers. Indeed, since the period of the principal root of any form f, as we saw in 5.4, depends on the cycle of the reduced forms of its class, if there are, let's say, l different cycle periods, then the numbers of the type $\frac{-b+\sqrt{D}}{2a}$ can only have these l periods, or half the length of these l periods.

Anyway, we stop delaying the promised demonstration:

Theorem 5.12. *Two reduced forms are equivalent if and only if they lie on the same cycle.*

Proof. Let $f = (a, b, c)$ and $f' = (a', b', c')$ be the two equivalent forms. We can suppose that a and a' are positive, because if for example a was negative we could consider, instead of f, one of the two adjacent forms of the same period, with opposite sign in the left term.

Let ω, ω' be the principal roots of f and f' respectively. From the previous assumptions and the definition of reduced forms, they are positive proper fractions. Since $f \sim f'$, there exists a properly equivalent transformation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ which converts f' into f, and therefore as usual

$$\omega' = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}.$$

By proposition 1.7, we can write

$$\omega' = [u; a_1 \cdots a_{2r}, v, \omega] = [u; a_1, \cdots, a_{2r}, (v + d_1), *d_2, \cdots, d_{2m}, *d_1],$$

where $\omega = [0; *d_1, \cdots, *d_{2m}]$, which is a pure periodic scf from proposition 5.9. If it happens that $v + d_1$ is negative, then by the method described in proposition 1.6 we can rewrite it as a scf. Thus, in every case we may write

$$\omega' = [\mu, l_1, l_2, \cdots],$$

where all the l_k are positive and μ is an integer.

Since ω' is the principal root of a reduced form with positive left term, we apply again proposition 5.9 and ω' must have a pure periodic scf and $0 < \omega' < 1$. Since an infinite scf is unique, $\mu = 0$ and $l_1, l_2, \cdots$ must be pure periodic. However, during the process that converted the first continued fraction of ω' into a simple one, only a finite number of partial quotients after $v + d_1$ were affected. Therefore, if we consider the period of ω and ω' starting form the first coefficient d_1 and l_1 respectively, then those periods only differ by a cyclical permutation. Moreover, from the way the rewriting was made, as we pointed, this cyclical permutation shifts the period of w an even number of partial quotients to form that of w'. We retain this fact.

So we act as follows: First we write $f := f_1 := (a, b, c)$ and we move forward in the cycle to get the coefficients $\delta_1, \delta_2 \cdots$, which satisfy $d_k = |\delta_k|$. Eventually, attending to the last paragraph, we will get $l_1, l_2, \cdots$, with $d_{k+2s} = l_k$ for some fixed natural s. Therefore, if we start to cycle from the form f_{2s+1} we get the coefficients $l_1, l_2, \cdots$, which means that, if we write the principal root of f_{2s+1} as w_{2s+1}, then $|\omega_{2s+1}| = \omega'$. But, since the sign of w_k alternates each step, we deduce that ω_{2s+1} is positive, as ω_1. Hence we can write $\omega_{2s+1} = \omega'$, and the forms f_{2s+1} and f' have the same principal root and discriminant, for $f_{2s+1} \sim f \sim f'$. Since they determine the form, it must be $f_{2s+1} = f'$, in other words, f' belongs to the same cycle as f, as we aimed to show.

□

5.4 Cycles and Pell's equation

Now we can prove some left propositions. We continue using the previous notation, where $f_1, \cdots, f_{2m}$ are the forms compounding the cycle and

$$N_{\delta_i} = \begin{pmatrix} 0 & 1 \\ -1 & \delta_i \end{pmatrix},$$

is the form which transforms f_i into f_{i+1}. We will suppose the form f_1 has principal root $\omega_1 > 0$, hence its pure periodic scf is

$$\omega_1 = [0; *\delta_1, -\delta_2, \cdots, \delta_{2m-1}, * - \delta_{2m}].$$

We will say it has convergents $R_n = \frac{P_n}{Q_n}$.

Lemma 5.13. *Denoting $N_{\delta_0} = Id$, for every $k \geq 0$ the following identity holds:*

$$M_k := N_{\delta_0} \cdots N_{\delta_k} = \begin{pmatrix} (-1)^{\frac{k(k+1)}{2}} P_{k-1} & (-1)^{\frac{(k+3)(k+4)}{2}} P_k \\ (-1^{\frac{k(k+1)}{2}}) Q_{k-1} & (-1)^{\frac{(k+3)(k+4)}{2}} Q_k \end{pmatrix}.$$

Proof. For $k \in [0, 3]$ it can be done easily, then we apply induction: if it is true for $4n, 4n+1, 4n+2$ and $4n+3$, using the definition of P_k and Q_k and multiplying the mentioned matrices, then the result follows for $4n+4, 4n+5, 4n+6$ and $4n+7$ after some tedious calculations.

□

Proposition 5.14. *For every discriminant $D > 0$, there exists a solution to positive Pell's equation, i.e. $Pell(D)$ contains non-trivial solutions.*

Proof. We consider the principal reduced form with discriminant D, I_p, and define f_1 as its right adjacent form, whose principal root ω_1 is positive. As it is defined in the previous lemma, the transformation M_{2m} cannot be the identity, for $m \geq 1$. Moreover, we also know that $f_1|_{M_{2m}} = f_1$, therefore M_{2m} is a non-trivial automorph. Using the correspondence between automorphs and $Pell(D)$, the result follows.

□

For the negative Pell's equation, we have the following one. We recall that I_p is the principal reduced form, whose principal root is ω_p.

Proposition 5.15. *For a positive discriminant D, there exists a solution of negative Pell's equation $x^2 - Dy^2 = -4$ iff the period as a scf of ω_p is odd.*

Proof. ($\Rightarrow$) If there exists a solution, there exists an antimorph for any form with discriminant D. We consider the principal reduced form I_p. Since I_p and its anti-form are equivalent, they also belong to the same cycle. Therefore using proposition 5.11 the scf of its principal root ω_p has odd period m.

($\Leftarrow$) If ω_p has odd period m, then we again consider F_p and it must have an antimorph. This antimorph has a corresponding solution of negative Pell's equation, which finishes the proof.

□

The period of the scf of ω_p has the same parity (actually it is just a cyclical permutation!) as the period of ω_D, the principal root of the principal form with discriminant D, which we named I_D. This can serve us to avoid calculating ω_p, which is more complicated than ω_D.

5.5 Summary

Let's summarize the main results of this chapter: for a given a positive discriminant D, there exists a finite number of reduced forms with such discriminant. Every form with discriminant D is properly equivalent to one reduced form. The reduced forms are not unique in $Cl(D)$, but they can be sorted into cycles so that two reduced forms belong to the same cycle iff they are equivalent.

Therefore, we can separate all the forms (a, b, c) with discriminant D into classes so that the representative of each class is one reduced form. In order to specify which one, although there are plenty of ways to do such a a choice, we can set we will choose the one with smallest b, and in case of two forms having the same center coefficient the one with the smallest $|a|$. Finally, if it coincides, the one with positive a.

Chapter 6

Degenerated cases

Now we are going to consider the degenerated cases which have been excluded so far.

6.1 Perfect square discriminant

Definition 6.1. *A form* (a, b, c) *with discriminant* h^2, $h > 0$, *is called* reduced *if*

$$a \in [0, h-1]; \quad b = h; \quad c = 0,$$

in other words if it has the form

$$(A, h, 0)$$

where $A \in [0, h-1]$.

Note that form the assumption of primitiveness, $(A, h) = 1$.

Obviously, if we are given $D = h^2$, the number of reduced forms with such discriminant is finite.

Proposition 6.2. *Every class in* $Cl(D)$ *contains at least one reduced form.*

Proof. Suppose we are given a form (a, b, c) with square discriminant h^2, $h > 0$. We aim to prove that there exists $(A, h, 0)$, $A \in [0, h-1]$, which is equivalent to the given one.

If $a = c = 0$, using

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

if $b = -h$, we are done. We assume they are not both zero. Applying T if necessary, let's say $a \neq 0$.

In this case we distinguish these two cases:

- If $b = h$, we must have $ac = 0$, hence $c = 0$. We define $A = a + hk$ where k is the unique integer so that $A \in [0, h-1]$. Since $(a, h, 0) \sim (A, \pm h, 0)$ via the transformation

  $$T^3 S^{-k} T = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix},$$

  we are done.

- If $b \neq h$, we define β, δ as coprime integers so that $\frac{\beta}{\delta} = \frac{(h-b)/2}{a}$. We can also find α, γ so that $\alpha\gamma - \beta\delta = 1$.
  Now we must note that it could happen $b = -h$ or $b \neq -h$. In the first case, $c = 0$, in the second one,

  $$\frac{(h-b)/2}{a} = \frac{c}{-(h+b)/2} = \frac{\beta}{\delta}.$$

  In both situations, if we apply the transformation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, the resultant form (a', b', c') satisfies the following equalities:
  $b' = b(\alpha\delta + \beta\gamma) + 2(a\beta\alpha + c\delta\gamma) =$
  $= b(\alpha\delta + \beta\gamma) + 2(\delta\frac{h-b}{2}\alpha - \beta\frac{h+b}{2}\gamma) = h(\alpha\gamma - \beta\delta) = h;$
  $c' = a\beta^2 + b\beta\delta + c\delta^2 =$
  $= \delta\beta\frac{h-b}{2} + b\beta\delta - \delta\beta\frac{b+h}{2} = 0.$
  Now, if $a' \in [0, h-1]$, then we are done setting $A = a'$. Otherwise we define $A = a' + hk$ where k is the unique integer so that $A \in [0, h-1]$ and apply the mentioned transformation $T^3 S^{-k} T$ to the form $(a', h, 0)$. This finishes the proof.

□

Actually since we only consider primitive forms, the case $A = 0$ only can happen when $(0, h, 0)$ is primitive, i.e. for $h = \pm 1$ and $D = 1$. So in general we can assert that every form f with discriminant $h^2 > 0$ has a primitive equivalent form $(A, h, 0)$ such that $A \in [1, h-1]$. Following the usual plot, now we want to show these reduced forms are unique.

Proposition 6.3. *Every class in $Cl(D)$ contains exactly one reduced form.*

Proof. Suppose we are given equivalent reduced forms $(a, h, 0)$ and $(a', h, 0)$. We aim to show they are identical. If there exists a transformation of the usual type satisfying $\alpha\gamma - \beta\delta = 1$, then the equivalence equations 2.1 give:

1. $a' = a\alpha^2 + h\alpha\gamma$
2. $h = h(\alpha\delta + \beta\gamma) + 2a\alpha\beta$
3. $0 = a\beta^2 + h\beta\delta$

Doing $(2) \times \beta - (3) \times 2\alpha$ we arrive to

$$h\beta = -h\beta(\alpha\gamma - \beta\delta) = -h\beta,$$

therefore $\beta = 0$. Since the determinant is 1, this implies $\alpha = \delta = \pm 1$. So (1) has the form

$$a' = a \pm h\gamma,$$

but this can only hold if $\gamma = 0$, for a and a' belong to $[0, h-1]$. So $a = a'$, and the given forms are identical, as desired.

□

All in all, we have showed that $Cl(D)$ is finite and we can choose the representative of every class to be its unique reduced form.

6.2 Zero discriminant

In this case most of the described properties are nonsense. Suppose we are given a form $f = (a, b, c)$ so that $b^2 - 4ac = 0$.

Proposition 6.4. *The form f is equivalent to either $(1, 0, 0)$ or $(-1, 0, 0)$.*

Proof. If $b = 0$ then a or c must be zero. Therefore the assumption of the primitiveness of the form implies the only two options are $f = \pm x^2$ and

$f = \pm y^2$. Since $(\pm 1, 0, 0) \sim (0, 0, \pm 1)$, the only two classes in this case are $(1, 0, 0)$ and $(-1, 0, 0)$, as desired.

If $b \neq 0$, we set $a \geq 0$, for the opposite follows analogously. Since $b^2 = 4ac$, we can write $b = 2B$, so $B^2 = ac$. Since we only consider primitive forms, a and c must be squares, hence we can write $a = A^2$; $c = C^2$ with adequate sign so that $B = AC$. So we have deduced that

$$ax^2 + bxy + cy^2 = (Ax + Cy)^2,$$

where A and C are coprime.

We can simplify these forms even more. We know there exist $\alpha, \gamma \in \mathbb{Z}$ such that $A\alpha + C\gamma = 1$. So we apply the equivalent transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & C \\ \gamma & A \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix},$$

which converts $Ax + Cy$ into x'. Hence if $a \geq 0$ then f is equivalent to $(1, 0, 0)$.

All in all, we deduce that f $= (a, b, c)$ with zero discriminant, a or c must be nonzero, let's say a. Then, if $a > 0$, this form is equivalent to $(1, 0, 0)$, and if $a < 0$, it is equivalent to $(-1, 0, 0)$, so we are done.

□

From last proposition we deduce that $Cl(D) = \{[(1, 0, 0)], [(-1, 0, 0)]\}$.

Chapter 7

Composition of forms

Now we assume we are given all the classes of forms of a fixed discriminant D. We aim to show a striking result first proved by Gauss, that they form a finite abelian group under a natural operation. Therefore, we must well-define what the composition of two forms is.

If f and f' are primitive forms of discriminant D, then a form F of the same discriminant is their composition if

$$f(x_1, y_1)f'(x_2, y_2) = F(X, Y),$$

where

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix},$$

for some $a_i, b_i, c_i, d_i \in A$ satisfying that all the 2×2-minors of this matrix have greatest common divisor 1. Therefore, whenever F is composed of f and f', every product of two numbers respectively represented by f and f' will be represented by F.

There are many equivalent ways to define an operation between forms producing the same group structure. We will choose Dirichlet's one, which is simple but has the disadvantage we just can define the operation for *united* forms.

Definition 7.1. *Two forms* (a_1, b_1, c_1) *and* (a_2, b_2, c_2) *are* united *if they have the same discriminant and*

$$\gcd(a_1, a_2, \frac{b_1 + b_2}{2}) = 1.$$

Note that b_1 and b_2 have the same parity since the given forms have common discriminant.

Given any two forms f, f_1, we will be interested in finding $f_2 \sim f_1$ so that f and f_2 are united. The following two results will let us do it.

Proposition 7.2. *A form $f(x, y)$ properly represents an integer m if and only if $f \sim (m, b, c)$ for some integers b, c.*

Proof. First we suppose that $f(p, q) = m$, where $\gcd(p, q) = 1$. There exist r, s so that $ps - qr = 1$, so we can do the following change of variable

$$f(px + ry, qx + sy) = f(p, q)x^2 + (2apr + bps + brq + 2cqs)xy + f(r, s)y^2 =$$

$$mx^2 + bxy + cy^2$$

which has the desired form.

To prove the converse we just have to note that the form $mx^2+bxy+cy^2$ properly represents m by taking $(x, y) = (1, 0)$, therefore also f, which is properly equivalent, properly represents m.

□

Proposition 7.3. *A primitive form $f = (a, b, c)$ can properly represent an integer which is relatively prime to a fixed number m.*

Proof. We will write $\pi(A, B, C)$ to refer to the product of all the primes dividing A, B and C. We will write $\pi(A, B, \neg C)$ to refer to the product of all the primes dividing A and B but not C. We consider

$$P = \pi(m, a, c); \quad Q = \pi(m, a, \neg c); \quad R = \pi(m, \neg a, c); \quad S = \pi(m, \neg a, \neg c)$$

They satisfy $PQRS = \pi(m, 0, 0)$ and they are pairwise coprime. Let's set $M = f(Q, RS)$, which is a primitive representation since
$\gcd(Q, RS) | \gcd(Q, R) \gcd(Q, S) = 1$. If we want to prove that M and m are coprime, we just have to check that if a natural number d divides M and one of P, Q, R, S, then it must be 1.

We will just do one example, the rest follow similarly. Suppose d divides Q and $M = aQ^2 + bQRS + c(RS)^2$. Then $d|c(RS)^2$, but by definition $d \nmid c$ and we said P, Q, R, S are pairwise coprime, thus $d = 1$, as desired.

□

Corollary 7.4. *Given $f = (a, b, c)$ and $f_1 = (a_1, b_1, c_1)$, there exists $f_2 = (a_2, b_2, c_2)$ so that $f_2 \sim f_1$ and $\gcd(a, a_2) = 1$.*

Proof. We choose any a_2 coprime to a_1. Using last proposition, it is properly represented by f_1, hence using the previous one we find the desired form f_2.

□

Proposition 7.5. *If (a_1, b_1, c_1) and (a_2, b_2, c_2) are united, then there exist integers B, C such that*

$$(a_1, b_1, c_1) \sim (a_1, B, a_2C)$$

$$(a_2, b_2, c_2) \sim (a_2, B, a_1C).$$

These two forms are also united.

Proof. It is enough to show that there exists an integer B so that this congruences are both satisfied

$$B \equiv b_1 \pmod{2a_1}$$

$$B \equiv b_2 \pmod{2a_2}$$

and also C is an integer (it is determined since we know the discriminant).

All the solutions to the first one have the form $b_1 + 2a_1\delta_1$. Hence, a sufficient and necessary condition to solve the two congruences simultaneously is that the following one is solvable

$$\frac{b_1 - b_2}{2} = -a_1\delta_1 \pmod{a_2}.$$

It has a solution iff $d := \gcd(a_1, a_2)$ divides $\frac{b_1-b_2}{2}$. But since

$$D = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2,$$

we deduce

$$\frac{b_1 + b_2}{2}\frac{b_1 - b_2}{2} = a_1c_1 - a_2c_2.$$

Since the forms are united, the last equation implies that d divides $\frac{b_1-b_2}{2}$, as desired.

Now we set $k = \operatorname{lcm}(a_1, a_2) = \frac{a_1a_2}{d}$. The integer B solution of the congruences above is unique modulo $2k$, so we can write $B = B_0 + 2kt$ with B_0 a fixed solution and arbitrary t. We need to choose a t so that

$$B^2 \equiv D \pmod{4a_1a_2}$$

to guarantee that C is an integer. The last congruence is equivalent to

$$B_0^2 + 4ktB_0 + 4k^2t^2 = D + 4a_1a_2m$$

for some integer m. Since $B_0^2 \equiv B^2 \pmod{D}$, we can divide by $4k$ and get the equivalent congruence

$$\frac{D - B_0^2}{4k} \equiv B_0 t \pmod{d}.$$

By the definition of B_0 and the united hypothesis, B_0 has an inverse modulo d, so we can write

$$t \equiv \frac{D - B^2}{4k} B_0^{-1} \pmod{d}.$$

We have uniquely determined t modulo d, therefore we have found all the possible B, which are unique modulo $2a_1a_2$.

It remains to show that these two forms are united. It follows from the congruences satisfied by B. If d divides B, a_1 and a_2, then it must also divide $\frac{b_1+b_2}{2}$, hence d must be 1. This finishes the proof.

□

So, given two united forms $f = (a_1, B, a_2C)$ and $f' = (a_2, B, a_1C)$, then under the transformation

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix}$$

we get the equation

$$(a_1{x_1}^2 + Bx_1y_1 + a_2C{y_1}^2)(a_2{x_2}^2 + Bx_2y_2 + a_1C{y_2}^2) = a_1a_2X^2 + BXY + CY^2.$$

In order to distinguish the forms f and f' from general united forms, we will say they are *prepared*. The product formula encourages us to state the following definition:

Definition 7.6. *The* compounded form *of the prepared forms $f = (a_1, B, a_2C)$ and $f' = (a_2, B, a_1C)$ is $F = (a_1a_2, B, C)$, what we will write as $F = f_1 \circ f_2$.*

However, this operation is really restricted. It is necessary to show that there exists a well-defined extension to the class group. That is our next step, for which we will need the following lemma.

Lemma 7.7. *Two forms (a_1, b_1, c_1) and (a_2, b_2, c_2) of the same discriminant are equivalent if and only if there exist integers α and γ such that*

$$a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 = a_2$$

$$2a_1\alpha + (b_1 + b_2)\gamma \equiv 0 \pmod{2a_2}$$
$$(b_1 - b_2)\alpha + 2c_1\gamma \equiv 0 \pmod{2a_2}.$$

Proof. Suppose the forms are equivalent using the change of variable $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Then by the equivalence equations 2.1 it is obvious that the desired α, γ are the ones in the matrix. The elements β and δ must satisfy

$$\alpha\delta - \beta\delta = 1$$

$$(b_1\gamma + 2a_1\alpha)\beta + (b_1\alpha + 2c_1\gamma)\delta = b_2.$$

We can write them as

$$\begin{pmatrix} \alpha & -\beta \\ b_1\gamma + 2a_1\alpha & b_1\alpha + 2c_1\gamma \end{pmatrix} \begin{pmatrix} \beta \\ \delta \end{pmatrix} = \begin{pmatrix} 1 \\ b_2 \end{pmatrix}.$$

So considering β and δ as unknowns, solving this system we arrive to

$$2a_1\alpha + (b_1 + b_2)\gamma = 2a_2\delta$$

$$(b_1 - b_2)\alpha + 2c_1\gamma = -2a_2\beta,$$

which finishes this part of the proof.

To prove the reciprocal we just have to go backwards from the given equations until we arrive to the equivalence equations, which is easy and we will omit.

□

Theorem 7.8. *Given the pairs of prepared forms*

$$f_1 = (a_1, B, a_2C), \quad f_2 = (a_2, B, a_1C)$$

$$f_3 = (m_1, N, m_2L), \quad f_4 = (m_2, N, m_1L),$$

and assuming $f_1 \sim f_3$ and $f_2 \sim f_4$, it also holds $f_1 \circ f_2 \sim f_3 \circ f_4$.

Proof. Using the previous lemma, we can find integers x_1, y_1 for the equivalence $f_1 \sim f_3$ so that

1. $a_1{x_1}^2 + Bx_1y_1 + a_2C{y_1}^2 = m_1$
2. $2a_1x_1 + (B + N)y_1 \equiv 0 \pmod{2m_1}$

3. $(B-N)x_1 + 2a_2Cy_1 \equiv 0 \pmod{2m_1}$

and integers x_2, y_2 for $f_2 \sim f_4$ so that

4. $a_2{x_2}^2 + Bx_2y_2 + a_2C{y_2}^2 = m_2$
5. $2a_2x_2 + (B+N)y_2 \equiv 0 \pmod{2m_2}$
6. $(B-N)x_2 + 2a_2Cy_2 \equiv 0 \pmod{2m_2}$.

We aim to show that there exist integers X, Y such that

7. $a_1a_2X^2 + BXY + CY^2 = m_1m_2$
8. $2a_1a_2X + (B+N)Y \equiv 0 \pmod{2m_1m_2}$
9. $(B-N)X + 2CY \equiv 0 \pmod{2m_1m_2}$.

Obviously we will set $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix}$. Let's check that it works.

It is clear that multiplying (1) and (4) we obtain (7). To deduce (8), we multiply (2) and (5) and, since f_1 and f_3 have the same discriminant D , we can substitute $N^2 \equiv B^2 - 4a_1a_2C \pmod{4m_1m_2}$.

Deducing (9) is not so simple. First we write

$$U := \frac{(B-\sqrt{D})}{2}X + CY.$$

The following four equations hold

$$[(B-\sqrt{D})x_1/2 + a_2Cy_1] \quad [a_2x_2 + (B+\sqrt{D})y_2] = a_2U$$
$$[a_1x_1 + (B+\sqrt{D})y_1] \quad [(B-\sqrt{D})x_2/2 + a_1Cy_2] = a_1U$$
$$[(B-\sqrt{D})x_1/2 + a_2Cy_1] \quad [(B-\sqrt{D})x_2/2 + a_1Cy_2] = (B-\sqrt{D})U/2$$
$$C[a_1x_1 + (B+\sqrt{D})y_1] \quad [a_2x_2 + (B+\sqrt{D})y_2] = (B+\sqrt{D})U/2.$$

We use the same process now, and substitute $N \equiv \sqrt{D} \pmod{4m_1m_2}$. Done this, all the left-hand sides are multiples of m_1m_2, thus so are the right-hand sides. We add up the last two equations and all in all we arrive to

$$a_2U \equiv a_1U \equiv BU \pmod{m_1m_2}$$

Since $\gcd(a_1, a_2, B) = 1$, this implies $U \equiv 0 \pmod{m_1 m_2}$. This implies

$$U = \frac{(B - \sqrt{D})}{2} X + CY \equiv \frac{(B - N)}{2} X + CY \equiv 0 \pmod{m_1 m_2}$$

which was the last congruence to be shown.

□

Now, using the common notation, we will write $[f]$ to refer to the class of the form f. When it does not lead to ambiguity, we will simply write (a, b, c) although we will be referring to the whole class.

The last theorem is strong enough to create a well-defined composition. Assume we are given any two forms f and f' with the same discriminant. Using corollary 7.4, there exists f'_1 so that $f' \sim f'_1$ and f and f'_1 are united. Using proposition 7.5, there exist f_p and f'_p so that $f \sim f_p$, $f' \sim f'_1 \sim f'_p$ satisfying that f_p and f'_p are prepared.

Then we can define

$$[f] \circ [f'] = [f_p] \circ [f'_p] := [f_p \circ f'_p],$$

where the first equality follows from the definition of class and the second one is well-defined from the last theorem.

It is natural to ask ourselves about the properties this composition has. We are going to prove it is associative, commutative, and also we are going to find the neutral and inverse elements.

Commutativity follows easily, for the composition of two prepared forms is not dependent on the arrangement of them.

We already proved that if the forms (a_1, b_1, c_1) have the same discriminant and also $a_1 = a_2$ and $b_1 \equiv b_2 \pmod{2a_1}$, then they are equivalent. We will use this result many times now.

To prove associativity, suppose we are given forms $f_i = (a_i, b_i, c_i), i \in [3]$ with the same discriminant. Using corollary 7.4 it is possible to find one equivalent form to f_2 so that $\gcd(a_1, a_2, a_3) = 1$, so all pairs of forms considered from now on will be united. We keep the name f_2 for this form and consider the composition

$$([f_1] \circ [f_2]) \circ [f_3] = (a_1 a_2, B, C) \circ (a_3, b_3, c_3) = (a_1 a_2 a_3, B', C').$$

Following the congruences of the proof of proposition 7.5, we can deduce

that, taking for granted the equality of discriminant, a necessary and sufficient condition for B' to make the last equalities hold are the congruences

$$B' \equiv b_i \pmod{2a_i} \quad i \in [3].$$

If we consider now the composition

$$[f_1] \circ ([f_2] \circ [f_3]) = (a_1, b_1, c_1) \circ (a_2 a_3, \beta, \gamma) = (a_1 a_2 a_3, \beta', \gamma'),$$

we arrive to the same congruences for β', so we deduce $B' \equiv \beta' \pmod{2a_1 a_2 a_3}$, which implies, with the fact that both forms have the same left term $a_1 a_2 a_3$, that they are equivalent. All in all, our composition is associative.

For the neutral element, first we note that $(1, b_1, c_1)$ and $(1, b_2, c_2)$ are equivalent iff they have the same discriminant, for $b_1 \equiv b_2 \pmod 2$. Thus they form one only class, which actually is the neutral element. Indeed, assuming we are given a form (a_2, b_2, c_2) we have

$$(1, b_1, c_1) \circ (a_2, b_2, c_2) = (1, B, a_2 C) \circ (a_2, B, C) = [(a_2, B, C)] = [(a_2, b_2, c_2)],$$

where the last equality follows from $B \equiv b_2 \pmod{2a_2}$. We will call the class of $(1, b_1, c_1)$ the principal class.

Finally, regarding the inverse element, given any form (a, b, c) we have

$$(a, b, c) \circ (a, -b, c) = (a, b, c) \circ (c, b, a) = [(ac, b, 1)],$$

where the last equality follows form the fact that b is actually one of the solutions of the congruences $x \equiv b \pmod{2a}$ and $x \equiv b \pmod{2c}$ and it makes the discriminant an integer, as desired. We have $(ac, b, 1) \sim (1, -b, ac)$, therefore we have proved that the inverse, or rather the opposed element of $[(a, b, c)]$ is $[(a, -b, c)]$.

Let's summarize all the previous results in the next major theorem.

Theorem 7.9. *Under the defined composition, the classes of forms of a fixed discriminant form a finite abelian group. The identity of the group is the principal class, and the inverse of the class of any form is the class of the opposite of the form.*

Chapter 8

Easy class groups

Now it is possible for us to determine, or at least study, some easy groups of classes. When writing the form (a, b, c) we will be referring to the class $[(a, b, c)]$.

Zero discriminant

In this case we have $Cl(0) = \{(1, 0, 0), (-1, 0, 0)\}$.These forms are already prepared, so our composition limits to multiplying the left coefficients. Thus,

$$Cl(0) \cong (\mathbb{Z}/3\mathbb{Z})^* \cong \{1, -1\},$$

where last two sets are provided with the usual product operation.

Square discriminant We will denote as $\Phi(h)$ the set of integers belonging to $[1, h]$ which are coprime to h.

When $D = h^2$, we proved that $Cl(D) = \{(A, h, 0)\}_{A \in \Phi(h)}$ provided $D > 1$. So the case $D = 1$ must be studied apart.

If $D = 1$, then $Cl(1) = \{(0, 1, 0)\}$. Indeed, $(0, 1, 0) \circ (0, 1, 0) = (0, 1, 0)$. Therefore $Cl(1)$ is the trivial group.

If $D = h^2 > 1$, as we said before, then $Cl(D) = \{(A, h, 0)\}_{A \in \Phi(h)}$. These forms are already prepared and again the only thing we do to multiply them is multiplying the first coefficients, i.e.

$$(A_1, h, 0) \circ (A_2, h, 0) = (A_1 A_2, h, 0).$$

Since $(1, h, 0)$ is the neutral element, we easily see

$$(Cl(h^2), \circ) \cong ((\mathbb{Z}/h\mathbb{Z})^*, \cdot)$$

via the isomorphism $\phi : (A, h, 0) \mapsto A$.

Definite case

The first thing we did when studying the forms with negative discriminant was to separate the positive from the negative ones since there was an obvious bijection

$$\phi : (a, b, c) \mapsto (-a, -b, -c)$$

between these two sets, such that there is no equivalence between them. This separation can be taken further.

Given a negative discriminant D, we consider $Cl(D)$. From now on, we will refer to the set of positive definite forms as $Cl^+(D)$ and to the class group of negative ones as $Cl^-(D)$. We have

$$Cl^+(D) \dot{\bigcup} Cl^-(D) = Cl(D).$$

Let's recall that the composition of two forms represents all the products between the numbers represented by these two forms. This implies that:

- If $f, g \in Cl^+(D)$, then $f \circ g \in Cl^+(D)$.
- If $f, g \in Cl^-(D)$, then $f \circ g \in Cl^-(D)$.
- If $f \in Cl^+(D)$ and $g \in Cl^-(D)$, then $f \circ g \in Cl^-(D)$.

The first deduction we can make is $Cl^+(D) \lhd Cl(D)$, for the class group is abelian. These fact together with the three stated properties imply that

$$Cl(D) \Big/ Cl^+(D) \cong (\mathbb{Z}/3\mathbb{Z})^*,$$

considering $(\mathbb{Z}/3\mathbb{Z})^*$ as a multiplicative group. Formally, this result comes from the morphism

$$\begin{aligned} \phi \colon Cl(D) &\to (\mathbb{Z}/3\mathbb{Z})^* \\ f &\mapsto 1 \text{ if } f \in Cl^+(D) \\ f &\mapsto -1 \text{ if } f \in Cl^-(D) \end{aligned}$$

so from $Cl(D)/\ker f \cong Imf$ we are done.

Part II

Forms with coefficients in $\mathbb{F}[T]$

Chapter 9

Preamble

In this chapter we will first study the structure of a ring of polynomials and some of its extensions, which will force us to expose the analogous tools to the ones we needed in $\mathbb{Z}$. This chapter is not necessarily involved in the theory of forms.

9.1 Extensions of a polynomial ring

Along this part of the present work we will work with the polynomial ring $\mathbb{F}_q[T]$, where $\mathbb{F}_q$ is a finite field of cardinal $q \in \mathbb{N}$ whose characteristic is not 2, in other words, q will be a power of an odd prime number. For the sake of briefness, we will write $A := \mathbb{F}_q[T]$.

Since we are not interested in the behavior of a polynomial $f(T) \in A$ as a function of T, but as an element of the ring A, we will simply denote $f(T)$ as f. The necessity of an analogous tool to the absolute value in $\mathbb{Z}$ motivates the following definition:

Definition 9.1. *The norm in A is the function*

$$\begin{aligned} |\cdot|\colon A &\to \mathbb{R} \\ 0 &\mapsto 0 \\ f &\mapsto q^{\deg f} \text{ provided } f \neq 0 \end{aligned}$$

The norm function satisfies the following properties:

1. $|f| \geq 0$ and $|f| = 0 \iff f = 0$.

2. $|f||g| = |fg|$
3. $|f+g| \leq \max\{|f|, |g|\}$, the equality holds if (but not only) $|f| \neq |g|$.

They are easy to prove. Property (3) implies

$$|f+g| \leq |f| + |g|,$$

hence the triangular inequality is satisfied and we can assert that A is a normed vectorial space over $\mathbb{F}_q$.

All these properties would hold if we had defined the norm of f using a different base from q. However, it is more convenient to define it this way in order to make the cardinal of (A/PA) be $|P|$, as it happens in $\mathbb{Z}$, although this fact will not be relevant for our purposes.

We will extend our norm function to the field of fractions the same way we would extend the absolute value to $\mathbb{Q}$.

First of all, we define $Q := \mathbb{F}_q(T)$, i.e. Q is the fraction field of A, whose elements will be called *rational functions*.

Definition 9.2. *The norm in Q is the function*

$$\begin{aligned} |\cdot| &: Q \to \mathbb{R} \\ f = \frac{a}{b} &\mapsto \frac{|a|}{|b|} \end{aligned}$$

It is easy to see that it is well-defined. This definition also satisfies the three properties stated before, hence the field Q is a normed vectorial space over $\mathbb{F}_q$ as well as A. This is specially interesting for it allows us to consider convergent sequences and Cauchy sequences, but first let's recall these definitions.

Definition 9.3. *A succession $(f_i)_{i\in\mathbb{N}}$ of rational functions is called a Cauchy sequence if*

$$\forall\, \epsilon > 0 \quad \exists N \text{ so that } n, m > N \Longrightarrow |f_n - f_m| < \epsilon.$$

Definition 9.4. *A succession $(f_i)_{i\in\mathbb{N}}$ of rational functions converges to $f \in Q$ if*

$$\forall\, \epsilon > 0 \quad \exists N \text{ so that } n > N \Longrightarrow |f_n - f| < \epsilon.$$

In other words, our idea of convergence is that for every $k \in \mathbb{N}_0$ the sequence $(\ [[x^k]]f_i\ )_{i\in\mathbb{N}}$ eventually stops changing, where $[[x^k]]f_i$ denotes the coefficient of x^k in f_i. In any normed space, as we know, convergent

sequences are also Cauchy. If we have the reciprocal result, we call this space *complete*. Although Q is not complete, we will include it into a bigger space R satisfying this property, as we do when including $\mathbb{Q}$ in $\mathbb{R}$. This aim takes us to the following definition:

Definition 9.5. *A Laurent series is a formal series of the kind*

$$\sum_{i=n}^{-\infty} a_i T^i = a_n T^n + \cdots + a_0 + \frac{a_{-1}}{T} + \cdots ,$$

where $a_i \in \mathbb{F}_q$ for every $i \in (-\infty, n]$.

There are many other possible definitions, but we have chosen this one to make the most of the parallelism between R and $\mathbb{R}$. The set of all Laurent series will be denoted as R. It is known that formal series can be summed and multiplied as follows (if the summation limits are not identical we can add zeros until they are so):

$$(\sum_{i=n}^{-\infty} a_i T^i) + (\sum_{i=n}^{-\infty} b_i T^i) = \sum_{i=n}^{-\infty} (a_i + b_i) T^i$$

$$(\sum_{i=n}^{-\infty} a_i T^i)(\sum_{i=n}^{-\infty} b_i T^i) = \sum_{i=2n}^{-\infty} c_i T^i$$

where $c_i = \sum_{k \leq n \text{ and } i-k \leq n} a_{i-k} b_k$.

It is also known (or anyway it can be easily proved) that, with these operations, R is a commutative field. The ring A is contained in R by means of the obvious isomorphism, hence the field Q also has an isomorphic field contained in R. From now on, we will abuse of the notation and consider $A \subset Q \subset R$. When we consider $f = \sum_{i=n}^{-\infty} a_i T^i$, we will suppose $a_n \neq 0$ unless otherwise is stated. We define $\deg f := n$, and $\operatorname{sgn} f := a_n$. They satisfy $\deg(fg) = \deg f + \deg g$ and $\operatorname{sgn}(fg) = \operatorname{sgn} f \operatorname{sgn} g$.

Definition 9.6. *The norm in R is the function*

$$\begin{aligned} |\cdot| \colon R &\to \mathbb{R} \\ 0 &\mapsto 0 \\ f &\mapsto q^{\deg f} \text{ provided } f \neq 0 \end{aligned}$$

It can be seen that the field R is a normed vectorial space over $\mathbb{F}_q$. Considering the multiplication algorithm in R it can be checked that under this definition the norm of every element in Q coincides with the one we stated previously, for $\deg(f^{-1}) = -\deg f$. The following result completely characterizes the aspect of Q in R. Regarding the notation, we say a Laurent series is periodic (of period p) if $a_{k+p} = a_k$ for every large enough k. We will also use "period" to refer to the word $(a_k \cdots a_{k+p})$.

Proposition 9.7. *A Laurent series is a rational function if and only if it is periodic.*

Proof. ($\Rightarrow$) Suppose f is rational, so we can write $f = \frac{p}{h}$ where $p, h \in A$. First it is convenient to study h^{-1}.

If we aim to find the inverse of $h = \sum_{i=0}^{n} b_i T^i$, we just have to go backwards in the multiplication algorithm, so let's write

$$1 = (\sum_{i=0}^{n} b_i T^i)(\sum_{i=0}^{-\infty} a_i T^i)$$

for some unknown $a_i \in \mathbb{F}_q$. Note that we do not need to justify a priori why we started from a_0, for the uniqueness of the inverse element implies that if we find one inverse we are done. The coefficients a_i must satisfy the following:

- $a_i = 0$ for $i \in \{0, \cdots, -n+1\}$
- $a_{-n} = {b_n}^{-1}$
- $a_i = -p_n^{-1}(\sum_{k=1}^{n} b_{n-k} a_{i+k})$ for $i \in \{-n-1, -n-2 \cdots\}$

Since it is possible to solve this equations, we have found an effective algorithm to find h^{-1}, as we aimed. But if we take a more careful look we notice that every a_i is determined by, at most, the n previous a_j. Since the field $\mathbb{F}_q$ containing all the a_i has q elements, there are q^n words of length n whose elements belong to $\mathbb{F}_q$. Therefore, if we consider the following set of words of length n

$$\{\ (a_{-i} \cdots a_{-i-n})\ \}_{i \in [0, q^n]}$$

applying the pigeonhole principle we deduce that at least two of those words must be identical. Since n elements completely determine the following ones, we have proved that h^{-1} has at most period q^n, where $n = \deg h$.

This was the difficult part: it can be easily seen that a periodic series maintains its period (both length and the word period) when it is multiplied by T or summed a constant, thus also ph^{-1} is periodic of period at most q^n.

($\Leftarrow$) Suppose $f = \sum_{i=n}^{-\infty} a_i T^i$ is periodic, or more detailedly, that $a_k = a_{k+p}$ for every $k \leq -M - 1$. Then we can write

$$T^M f = g + \frac{1}{T^p} \sum_{i=0}^{\infty} h T^{-ip}$$

for some adequate $g, h \in A$. Since

$$\sum_{i=0}^{\infty} T^{-ip} = \frac{1}{1 - T^{-p}},$$

it follows that we can write f as a quotient of elements of A, as we aimed to prove.

□

As a consequence, Q is strictly contained in R. The elements belonging to R but not Q are called *irrational functions*. Last result also helps us to prove the incompleteness of Q, for example by considering the sequence

$$(f_n)_{n \in \mathbb{N}} \text{ where } f_n := \sum_{i=0}^{-n} i T^{-i}.$$

It remains to prove what we promised about the set R of Laurent series, its completeness. Let's go for it.

Proposition 9.8. *With the defined norm $|\cdot|$, R is complete.*

Proof. We consider the Cauchy sequence $(f_i)_{i \in \mathbb{N}}$, where all $f_i \in R$. This means that for every $k \in \mathbb{N}$ there exists N_k such that $|f_n - f_m| < q^{-k}$ for every $n, m \geq N_k$.

In other words, for every $n, m \geq N_k$ the formal series f_n and f_m coincide at least until the coefficient T^{-k}. We define $a_{-k} := [[T^{-k}]] f_{N_k}$.

Now we set $k = 1$ and $S = \deg(f_{N_1})$. If $S < 0$, we do nothing. Otherwise for every $k \in [0, S]$ we define $a_k := [[T^k]] f_{N_1}$.

We claim that the given sequence has a limit, which is $f = \sum_{i=S}^{-\infty} a_i T^i$. Indeed, for every $\epsilon > 0$ we choose a k such that $q^{-k} < \epsilon$, and then for every

$n \geq N_k$ the inequality

$$|f - f_n| < \epsilon$$

holds attending to the definition of f. Since obviously $f \in R$, we deduce that R is complete, as desired.

□

Along this work a particular kind of irrational functions will turn out to have big importance, the square roots.

Given $f \in R$, if there exists $g \in R$ such that $g^2 = f$ we will call g a *square root of* f. It is convenient to state a definition before next result.

Definition 9.9. *We say a series $f \in R$ is a* plant *if* $\deg f$ *even and* $\operatorname{sgn} f \in {\mathbb{F}_q*}^2$.

Proposition 9.10. *A series $f \in R$ has a square root iff f is a plant.*

Proof. ($\Rightarrow$) It follows from $\deg f^2 = 2 \deg f$ and $\operatorname{sgn} f^2 = (\operatorname{sgn} f)^2$.

($\Leftarrow$) Without loss of generality we can suppose $\operatorname{sgn} f = 1$. If $f = \sum_{i=2n}^{-\infty} b_i T^i$, we aim to find $g = \sum_{i=n}^{-\infty} a_i T^i$ such that $g^2 = f$. Since $b_{2n} = 1$, if we assume $a_n = 1$ then the condition $g^2 = f$ is equivalent to the following equations :

- $a_n = 1$
- $a_{n-k} = \frac{1}{2}(f_{2n-k} - \sum_{i=1}^{k-1} a_{n-i} a_{-k+i})$ for every $k \in \mathbb{N}$

This is an effective algorithm to calculate the square root of the plant f. We have assumed that $a_n = 1$, although we may have assumed $a_n = -1$. These are the only two possible options, therefore there exist exactly two square roots of the plant f provided it is not zero (in that case the square root is unique). In particular, every plant has at least one square root, as we aimed to prove.

□

From now on we will use the word "plant" when the considered element is not a perfect square, and the word "square" when it is.

We miss another fundamental tool when studying properties of $\mathbb{Q}$ as a subset in $\mathbb{R}$, the floor function.

Definition 9.11. *The floor function in R is the function*

$$\begin{aligned} \lfloor \cdot \rfloor \colon R &\to A \subset R \\ f &\mapsto 0 \text{ if } \deg f < 0 \\ f = \sum_{i=n}^{-\infty} a_i T^i &\mapsto \sum_{i=n}^{0} a_i T^i \text{ otherwise} \end{aligned}$$

The floor function has the following basic properties:

- $\lfloor z + a \rfloor = \lfloor z \rfloor + a$ for every $a \in A$.
- $\lfloor \alpha z \rfloor = \alpha \lfloor z \rfloor$ for every $\alpha \in \mathbb{F}_q$.
- If $p, q \in A$, then $\lfloor p/q \rfloor$ equals the euclidean quotient of p over q.
- If $\lfloor z \rfloor = 0$ and $z \neq 0$ then $\lfloor 1/z \rfloor \neq 0$.
- $\lfloor z \rfloor = 0$ iff $|z| < 1$.

All in all, we have reached our purpose of creating an environment such as that of real numbers. As in that case, we need an alternative less arbitrary representation of Laurent series which better expresses the behavior of irrational functions in R. This desire takes us to the following item.

9.2 Continued fractions

Our exposition of continued fractions in R will not differ too much from the one we would give for $\mathbb{R}$. This happens because just elemental algebraic manipulation are necessary in order to prove most of results, hence we can talk about continued fractions in a wider context where we just consider a normed domain whose fraction field has been metrically completed and provided with a well-behaved ceiling function which maps the complete field into the domain. The points where we will explain more details will be those related to convergence.

Definition 9.12. *A finite continued fraction is an expression*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_N}}}$$

provided it is defined, where all $a_i \in R$.

We will more briefly write this expression as $[a_0; \cdots, a_N]$, separating the first term from the rest with a semicolon. If $a = [a_0; \cdots, a_N]$ we will say this is an expression of a as a continued fraction, or alternatively we will say that it represents a. The a_i are the *partial quotients* of the continued fraction. The n-th convergent of this expansion is

$$R_n = [a_0; \cdots, a_n], 0 \leq n \leq N,$$

provided it is defined. If we define

$$P_{-1} := 1; \quad P_0 := a_0; \quad P_n := a_n P_{n-1} + P_{n-2} \text{ for } n \geq 1$$

and

$$Q_{-1} := 0; \quad Q_0 := 1; \quad Q_n := a_n Q_{n-1} + Q_{n-2} \text{ for } n \geq 1$$

then we can state this result:

Proposition 9.13. *The following equalities hold:*

- $R_n := [a_0; \cdots, a_n] = \frac{P_n}{Q_n}$ *for* $n \geq 0$.
- $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$, *for* $n \geq 0$.
- $\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_{n-1} Q_n}$ *for* $n \geq 0$.

Proof. Both follow by induction. The case $n = 0$ is obvious.

(1) We have

$$[a_0; \cdots, a_n, a_{n+1}] = [a_0; \cdots, a_n + 1/a_{n+1}],$$

we apply the induction hypothesis and it becomes

$$\frac{(a_m + 1/a_{m+1}) P_{m-1} + P_{m-2}}{(a_m + 1/a_{m+1}) Q_{m-1} + Q_{m-2}},$$

which can be easily converted into $\frac{P_{n+1}}{Q_{n+1}}$

(2) Applying the definitions we easily get

$$P_{n+1} Q_n - P_n Q_{n+1} = -(P_n Q_{n-1} - P_{n-1} Q_n).$$

(3) We just need to divide the previous equation by $Q_n Q_{n-1}$.

□

Definition 9.14. *A finite simple continued fraction (finite scf) is a finite continued fraction* $[a_0; \cdots a_N]$ *where* $a_0 \in A$ *and* $\forall n \in [1, N] \quad a_n \in A$ *and* $|a_n| > 1$.

Obviously every finite scf represents a rational function, and conversely every rational function is represented by a finite scf, which we will prove later. One of the virtues of the finite scf's is that they are unique:

Proposition 9.15. *If two finite scf's represent the same element in R, then they are identical.*

Proof. We assume $[a_0; \cdots, a_N] = [b_0; \cdots, b_M]$ and without loss of generality suppose $N \leq M$. By induction, it can be easily seen that $\deg [0; a_n, \cdots, a_N] \leq -1$ for every $1 \leq n \leq N$, and we can assert the analogous property for the other scf. Taking $n = 1$, we have $a_0 = b_0$. We invert both sides and continue the process. If $N = M$, we are done. Otherwise we will arrive to $0 = [0; b_{N+1} \cdots, b_M]$ which is an absurd. This finishes the proof.

□

We can say more about finite scf's.

From the definition of P_n and Q_n we can deduce that, for every $n \geq 1$,

$$|P_{n+1}| > |P_n| \, ; |Q_{n+1}| > |Q_n|,$$

which means that the degree of these polynomials is increasing.

From equation

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$$

it follows that the convergent $R_n = \frac{P_n}{Q_n}$ is well written, i.e. its numerator and denominator are coprime.

And finally the equation

$$R_n - R_{n-1} = \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_{n-1} Q_n}$$

asserts that the difference between two consecutive convergents has decreasing norm, which implies that the sequence R_n converges.

Last property is specially interesting for it suggests the possibility of extending the definition of finite scf the same way we would do it in $\mathbb{R}$.

Definition 9.16. *Given $\{a_i\}_{i\in\mathbb{N}_0}$ where $a_0 \in A$ and $\forall n \in \mathbb{N}$, $a_n \in A$ and $|a_i| > 1$, an infinite simple continued fraction (infinite scf) is a notational expression $[a_0; a_1, \cdots]$ whose value equals the limit*

$$\lim_{n\to\infty} R_n,$$

where $R_n = [a_0; \cdots, a_n]$.

Although this definition seems quite formal, in general we will operate with infinite scf's the same way we would do with finite ones, for all the simple algebraic properties work the same way in both cases. But first it is recommendable to check they are unique:

Proposition 9.17. *If two infinite scf's represent the same element in R, then they are identical.*

Proof. We define $S_n = [a_n; a_{n+1}, \cdots]$ and $R_m^n = [a_n; \cdots, a_{n+m}]$. We claim that $\deg S_n \geq 1\ \forall n \in \mathbb{N}$.

It can be easily proved by induction that $\deg R_m^n \geq 1$ for all $n \in \mathbb{N}$. So we do

$$\deg S_n = \deg \lim_{m\to\infty} R_m^n = \lim_{m\to\infty} \deg R_m^n \geq 1.$$

It is easy to check that limit and degree can be swapped in the second equality.

Now we can prove the proposition: suppose $[a_0; a_1, \cdots] = [b_0; b_1, \cdots]$. Since $\deg [0; a_1, \cdots] \leq -1$ and $\deg [0; b_1, \cdots] \leq -1$, we have $a_0 = b_0$. We manipulate the equality and get $[a_1; a_2, \cdots] = [b_1; b_2, \cdots]$. So we can apply strong induction and the proposition is proved.

□

It remains to show the exhaustiveness of the scf's (we include finite and infinite ones), which is our next step.

Given any $x \in R$, the following algorithm lets us finding its scf. We define a_i, X_i, Z_i by

$$a_0 = \lfloor x \rfloor; \quad Z_0 = x - a_0,$$

$$X_i = \frac{1}{Z_{i-1}}; \quad a_i = \lfloor X_i \rfloor; \quad Z_i = X_i - a_i \quad i \geq 1$$

The algorithm continues as long as $Z_i \neq 0$. They satisfy $x = [a_0; \cdots, a_{i-1}, X_i]$, where X_i is not necessarily a polynomial. If $x \in Q$, then the algorithm is

a rephrasing of the euclidean algorithm to divide two polynomials $p, q \in A$ and it eventually finishes producing the scf expression of x. If $x \in R \setminus Q$, then the process never finishes. However, we have this result:

Proposition 9.18. *With the previous notation, if x is an irrational function, $x = [a_0; a_1, \cdots]$.*

Proof. We consider the scf $x = [a_0; \cdots, a_{i-1}, X_i]$ and $R_{i-1} = [a_0; \cdots, a_{i-1}]$. Since the $\deg X_i \geq 1$, we can assert that

$$x - R_i = \frac{1}{Q_{i-1}Q'_{i-1}}$$

where Q_{i-1} is the denominator of the last convergent of R_{i-1} and Q'_{i-1} is the denominator of the last convergent of $[a_0; \cdots, a_{i-1}, X_i]$, which is not a scf but it is easy to see that $\lim_{i\to\infty} \deg Q'_{i-1} = \infty$, as it happens with Q_{i-1} (actually it is enough to have $\lim_{i\to\infty} \deg Q_{i-1} = \infty$ and $\deg Q'_i$ greater than some constant).

Anyway, it follows that $\lim_{i\to\infty} x - R_i = 0$, as we wanted to prove.

□

In most of cases we will consider scf's of the following type:

Definition 9.19. *The scf $[a_0; a_1 \cdots]$ is called* periodic *(of period p) if there exist integers I, p so that $a_i = a_{i+p}$ for all $i \geq I$, and we will write*

$$x = [a_0; \cdots a_{I-1}, *a_I, \cdots, *a_{I+p-1}],$$

where the $*$ indicates the period. We will also refer to the ordered set $\{a_I, \cdots, a_{I+p-1}\}$ as the period *of the previous periodic scf.*

If $a_0 = 0$ and $I = 1$, we will say the scf is pure periodic.

Later, with more adequate tools, we will prove that periodic scf's are those series $x \in R$ such that they satisfy $ax^2 + bx + c = 0$, where $a, b, c \in A$ and $a \neq 0$. Note that, since $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, it will be necessary that $b^2 - 4ac$ is a plant.

It remains to expose some particular results we will need:

Proposition 9.20. *Let $x, y \in R$. If there exist $\alpha, \beta, \gamma, \delta \in A$ so that $\alpha\delta - \beta\gamma = 1$ and*

$$y = \frac{\alpha x + \beta}{\gamma x + \delta},$$

then we can express y as

$$y = \psi^2[u; a_1, \cdots, a_r, v, x],$$

where $\psi \in \mathbb{F}_q^*$, $a_1, \cdots, a_r \in A$ satisfy $|a_i| > 1$ and $u, v \in A$.

Proof. If any of $\alpha, \beta, \gamma, \delta$ is zero, the result follows easily. Otherwise, we redefine the coefficients multiplying α and δ by a constant and dividing the other two by this constant, in order to make $\operatorname{sgn}\alpha \in 1$, which is why ψ^2 makes appearance. Let u be defined as $u := \lfloor \beta/\delta \rfloor$, so $\beta/\delta - u$ is a proper fraction (i.e. its degree is less than 0). So if we expand β/δ into a scf, it gives

$$\frac{\beta}{\delta} = [u; a_1, \cdots, a_r],$$

where each a_i satisfies $|a_i| > 1$. Now suppose P/Q is the penultimate convergent of this scf. Then from proposition 9.13 we have

$$\beta Q - \delta P = (-1)^r,$$

and on the other hand $\beta\gamma - \delta\alpha = 1$. In other words, we have the solutions $(x, y) = ((-1)^r Q, (-1)^r P)$ and $(x, y) = (-\gamma, \alpha)$ of equation $\beta x - \delta y = 1$. From Bachet's identity, this two solutions must satisfy

$$\alpha = (-1)^r P + (-1)^r v\beta; \quad \gamma = (-1)^r Q + (-1)^r v\delta$$

for some $v \in A$. So this gives

$$\alpha/\gamma = [u; a_1, \cdots, a_r, v],$$

so from the definition of the partial quotients we finally deduce

$$\frac{y}{\psi^2} = \frac{\alpha x + \beta}{\gamma x + \delta} = [u; a_1, \cdots, a_r, v, x],$$

as we wanted to prove.

□

Lemma 9.21. *If the infinite continued fraction $x = [a_0; a_1, \cdots]$ is a scf except for $a_r \in \mathbb{F}_q^*$, then it is possible to convert it into a scf as the following one:*

$$x = \pm\psi^2[a_0'; \cdots, a_{r-2}', a_{r-1}', a_r', a_{r+2}, \cdots],$$

where $\psi \in \mathbb{F}_q$.

Proof. If follows from $[b_0, b_1, b_2, b_3, \frac{1}{z}] = [b_0, b_1 + b_2^{-1}, -b_2^2 b_3 - b_2, \frac{1}{-b_2^2 z}]$, where we supposed $b_2 \in \mathbb{F}_q^*$.

□

Corollary 9.22. *If the series $\omega \in R$ and $\Omega \in R$ satisfy*

$$\omega = \frac{\alpha\Omega + \beta}{\gamma\Omega + \delta},$$

where $\alpha, \beta, \gamma, \delta \in A$ and $\alpha\delta - \beta\gamma = 1$, then, if Ω has a periodic scf of the form $[t_0; t_1, \cdots, t_m, *r_1, \cdots, *r_p]$ then there exists $\psi \in \mathbb{F}_q^*$ such that

$$\omega = \pm\psi^2[a_0; \cdots, a_M, *r_1, \cdots, *r_p]$$

for some M and some $a_i \in A$ such that $|a_i| > 1$.

9.3 The modular group

The following definition works for any ring A, but we recall that $A = \mathbb{F}_q[T]$.

Definition 9.23. *The group $SL(2, A)$ is the multiplicative group of the 2×2-matrices with coefficients in A and determinant 1.*

The following matrices are important elements of $SL(2, A)$

$$S_k := \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \text{ where } k \in A,$$

$$U_\psi := \begin{pmatrix} \psi & 0 \\ 0 & \psi^{-1} \end{pmatrix} \text{ where } \psi \in {\mathbb{F}_q}^* \text{ and}$$

$$T := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

for we have the following result:

Proposition 9.24. *The group $SL(2, A)$ is generated by its elements $\{S_k\}_{k\in A}$, $\{U_\psi\}_{\psi\in{\mathbb{F}_q}^*}$ and T.*

Proof. Suppose we are given $M := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. We will multiply it on the left until we reach the identity.

If $\beta \neq 0$, since $S_k M = \begin{pmatrix} \alpha + k\gamma & \beta + k\delta \\ \gamma & \delta \end{pmatrix}$, after applying T if necessary we can choose $k \in A$ so that $|\beta + k\delta| < |\delta|$. We use T to swap the rows and

repeat the process until we arrive to a matrix where the upper right element is zero, therefore it must be of the form

$$\begin{pmatrix} \chi & 0 \\ w & \chi^{-1} \end{pmatrix}.$$

We multiply by $T^3 S_{\chi w} T U_{\chi^{-1}}$ and we are done.

□

Actually, last proposition can be sharpened not considering all U_ψ with $\psi \in {\mathbb{F}_q}^*$ but just a fixed one U_{ψ_0}, provided ψ_0 generates the cyclic group $({\mathbb{F}_q}^*, \cdot)$. This implies that $< U_{\psi_0} >= \{U_\psi\}_{\psi \in {\mathbb{F}_q}^*}$.

We need a brief proposition before finishing:

Proposition 9.25. *Given a field $\mathbb{F}_q$ whose characteristic is not 2, there exists at least one element $\mu \in \mathbb{F}_q$ which is not a square. If we define $I := \{a^2 \,|a \in {\mathbb{F}_q}^*\}$, then ${\mathbb{F}_q}^* = I \sqcup \mu I$*

Proof. We consider the function

$$\begin{aligned} f \colon {\mathbb{F}_q}^* &\to I \\ a &\mapsto a^2 \end{aligned}$$

The antiimage of one element $f(a)$ are the elements a and $-a$. Therefore $|I| = \frac{{\mathbb{F}_q}^*}{2}$. Thus at least one non square element μ exists. Finally, the well-defined function

$$\begin{aligned} \phi \colon I &\to {\mathbb{F}_q}^* - I \\ a^2 &\mapsto a^2 \mu \end{aligned}$$

is a bijection, therefore attending to the cardinal of these sets it must be ${\mathbb{F}_q}^* = I \sqcup \mu I$

□

We will usually consider μ, a fixed non square of ${\mathbb{F}_q}^*$.

Chapter 10

Fundamental tools

A quadratic binary form with coefficients in $A := \mathbb{F}_q[T]$, or more briefly from now on a form, is an homogeneous polynomial

$$f(X, Y) = aX^2 + bXY + cY^2$$

where $a, b, c \in A$. The form $f(X, Y)$ will be denoted when convenient as $f = (a, b, c)$.

A form f is said to be *primitive* if $\gcd(a, b, c) = 1$. We will limit our work to these forms.

Definition 10.1. *The discriminant D of the form (a, b, c) is the polynomial $D = b^2 - 4ac$.*

We could have forced our binary forms to have the form $aX^2 + 2bXY + cY^2$. In such a case, it is better to define the discriminant as $b^2 - ac$. We have not chosen this convention because we want to take advantage of the existent parallelism between forms with coefficients in $\mathbb{Z}$ and those with coefficients in A.

Given any polynomial D, there exists at least one binary form with that discriminant, such as the form $I_D = (1, 0, -\frac{D}{4})$, which is called the *principal form* with that discriminant.

A form $f(X, Y)$ represents a polynomial m if there exist polynomials X_0, Y_0 so that $f(X_0, Y_0) = m$. If $\gcd(X_0, Y_0) = 1$ we will say such a representation is *primitive*.
In order to consider the form $f = (a, b, c)$ and all polynomials represented by it, we write $f(X, Y) = m$. We can complete the square to obtain

$$4am = (2aX + bY)^2 - DY^2 \tag{10.1}$$

The analogy between this case and the one in $\mathbb{Z}$ suggests the possibility of considering the following distinctions, which will be studied later:

- If $\deg D$ is odd, we will say we are considering *the imaginary case*.
- If $\deg D$ is even and $\operatorname{sgn} D$ is not a square, we will call it *the pseudo-imaginary case*. In this case, the polynomials represented by $f = (a, b, c)$ have degree of the same parity as a, as it can be easily deduced from equation 10.1.
- If $\deg D$ is even, $\operatorname{sgn} D$ is a square but D is not a perfect square, this one will be referred as *the real case*. When we say D is a plant we will be referring to this case exclusively, and not the following one.
- If D is a perfect square, we will call it *the square case*, and we will say D is a square.

Now we are going to introduce the transformations between forms. We consider the form $f = (a, b, c)$, with discriminant D, and the form $f' = (a', b', c')$.

The *matrix of* f is $A_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$, whose coefficients belong to A.

Let's recall that the group $SL(2, A)$ is the multiplicative group of the 2×2-matrices with coefficients in A and determinant 1.

Definition 10.2. *The forms f and f' are* equivalent *if there exists a transformation $M \in SL(2, A)$ such that $M^T A_f M = A_{f'}$, what we will write as $f \sim f'$, or more precisely as $f|_M := f'$.*

It is straightforward to see that this is an equivalence relation, which we will write as $f \sim f'$. Since $\det M = 1$, if two forms are equivalent, then they have the same discriminant.

In other words, f and f' are equivalent if there exist $\alpha, \beta, \gamma, \delta \in A$ so that $\alpha\delta - \beta\gamma = 1$ and

$$f(\alpha X + \beta Y, \gamma X + \delta Y) = f'(X, Y).$$

We can rewrite last equation as

$$f(\alpha, \gamma)X^2 + [b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta)]XY + f(\beta, \delta)Y^2 = f'(X, Y).$$

Therefore, a' and c' can be represented by f, and also we have the following equations, which we will refer as *equivalence equations*:

$$\begin{aligned} a\alpha^2 + b\alpha\gamma + c\gamma^2 &= a' \\ b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta) &= b' \\ a\beta^2 + b\beta\delta + c\delta^2 &= c' \end{aligned} \tag{10.2}$$

It there exists a transformation from f to f' with determinant -1, we will say they are improperly equivalent. Note that this is not an equivalence relation.

As we proved in the preamble, the group $SL(2, A)$ is generated by its elements $\{S_k\}_{k\in A}, \{U_\psi\}_{\psi\in\mathbb{F}_q{}^*}$ and T, defined as

$$S_k := \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix};\ U_\psi := \begin{pmatrix} \psi & 0 \\ 0 & \psi^{-1} \end{pmatrix};\ T := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

These three generators act as follows on a form (a, b, c) :

- $S_k : (a, b, c) \longmapsto (a, b + 2ak, ak^2 + bk + c)$
- $U_\psi : (a, b, c) \longmapsto (a\psi^2, b, \frac{c}{\psi^2})$
- $T : (a, b, c) \longmapsto (c, -b, a)$

Given $D \in A$, the group $SL(2, A)$ acts on the right on the set of forms of discriminant D. The action of M on a form with matrix A_f produces a form $f|_M$ with matrix $M^T A_f M$. The orbits of this action are the classes of forms under the equivalence relation "$\sim$."

Since M and $-M$ act identically on a form f, in order to identify them we define

$$PSL(2, A) := SL(2, A)/\{\pm\mathrm{Id}\},$$

which is the *modular group* we will use from now on. Therefore the transformations matrices will be considered as matrices whose sign may change conveniently.

Let's expose briefly some useful equivalences:

Doing $x = y'$ and $y = x'$, we see that (a, b, c) and (c, b, a) are improperly equivalent. We will say (c, b, a) is the *associated form* of (a, b, c).

By applying T to (c, b, a) and using last result we see the forms (a, b, c) and $(a, -b, c)$ are improperly equivalent. We say these two forms are *opposed*.

Another frequently used equivalence will be that of adjacent forms:

Definition 10.3. *The forms $f = (a, b, c)$ and $f' = (a', b', c')$ are* adjacent*, or more precisely the form f' is right adjacent to the form f, if they satisfy the following three properties:*

- *They have the same discriminant.*
- $a' = c \neq 0$.
- $b' \equiv -b \pmod{2c}$.

In this case we will also say that the form f is left adjacent to the form f'.

If f' is right adjacent to the form f then the following matrix transforms f into f':

$$N_\delta := TS_\delta = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix},$$

where δ is defined as $\delta = \frac{b+b'}{2c}$.

This type of transformation N_δ converts a form (a, b, c) into

$$(c, -b + 2c\delta, c\delta^2 - b\delta + a).$$

Definition 10.4. *We shall call a form* (a, b, c) ambiguous *if a divides b.*

The same way as in $\mathbb{Z}$, ambiguous forms are improperly equivalent to themselves, and also (a, b, c) and (c, b, a) are adjacent iff (a, b, c) is ambiguous.

Since the group $PSL(2, \mathbb{Z})$ acts on the right on the set of forms of discriminant D, given a form f we can consider its stabilizer subgroup, i.e. the transformations $M \in PSL(2, \mathbb{Z})$ such that $f|_M = f$. Those transformations will be called *automorphs of f* and the stabilizer group of f as $Aut(f)$.

Similarly, we define an *μ-morph* of a form (a, b, c) as a transformation M such that $f|_M = (\mu a, b, \frac{1}{\mu}c)$.

10.1 Principal root

As we mentioned in the preamble, just plants and squares have square roots in R. Therefore the concepts of this section will be related only to the real

case, and from now on we will implicitly assume that all forms considered have plant discriminant. Given a plant D with sign ρ^2, when writing $\sqrt{D}$ we will be referring only to the root with sign ρ.

Definition 10.5. The principal root *of a form* (a, b, c) *is*

$$\omega = \frac{-b + \sqrt{D}}{2a} \in R$$

Since 1 and $\sqrt{D}$ are Q-independent, we can state the following result we had in $\mathbb{Z}$:

Proposition 10.6. *Two forms with plant discriminant D and the same principal root are identical.*

Proof. Suppose the mentioned forms are $f = (a, b, c)$ and $f' = (a', b', c')$. We have

$$\frac{-b + \sqrt{D}}{2a} = \frac{-b' + \sqrt{D}}{2a'}.$$

Multiplying both sides by $2aa'$ and equaling the Q-lineally independent terms, we get the two equations

$$a'b = b'a; \quad a' = a,$$

so $b = b'$. Using the equality of discriminant we arrive to $c' = c$.

□

And we can also state the following one, whose proof is identical to the one in $\mathbb{Z}$:

Proposition 10.7. *If the forms f, f' are properly equivalent via the transformation $M := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, i.e. if $f|_M = f'$, and their principal roots are ω and ω' respectively, then they satisfy*

$$\omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta}.$$

Conversely, if the principal roots of f and f' satisfy the mentioned equation and $\alpha\delta - \beta\gamma = 1$, then the forms f and f' are properly equivalent via M.

10.2 Automorphs and Pell's equation

We will refer to any of the equations

$$x^2 - Dy^2 = \psi^2 \text{ where } \psi \in (\mathbb{F}_q)^*$$

as a Pell's equation, and to any of the equations

$$x^2 - Dy^2 = \mu\psi^2, \text{ where } \psi \in (\mathbb{F}_q)^*,$$

as a μ-Pell's equations. Recall that μ is a fixed non-square of $(\mathbb{F}_q)^*$.

Definition 10.8. *We will write $(x, y) \sim (\psi^2 x, \psi^2 y)$ for every $\psi \in (\mathbb{F}_q)^*$. Since $\sim$ is an equivalence relation, from now on the representative of each call will be the pair (x, y) such that $\operatorname{sgn} x = 1$.*

From now on, when considering the pair (x, y), we will be actually referring to its class.

Definition 10.9. *The set $Pell(D)$ is the set of all solutions $(x, y) \in A \times A$ to some Pell's equation. The solution $(1, 0) \in Pell(D)$ is called the trivial solution.*

Similarly, the set $\mu Pell(D)$ is the set of all solutions $(x, y) \in A \times A$ to some μ-Pell's equation.

At first glance we deduce that:

- If $|D| = 0$, then $Pell(D) = \{(1, y)\}_{y \in A}$.
- If $\deg D$ is odd then $Pell(D) = \{(1, 0)\}$.
- If $D = h^2$ where $|h| > 1$ equation $(x + hy)(x - hy) = \psi^2$ has just the trivial solution, hence $Pell(D) = \{(1, 0)\}$.

Similarly, $\mu Pell(0) = \{\emptyset\}$ and also $\mu Pell(h^2) = \{\emptyset\}$.

We are more interested in the cases where D is a plant, which is the case we will be considering from now on.

As it happens in $\mathbb{Z}$, if (a, b) and (c, d) are solutions to some Pell's equation, then if we define $(x, y) \in A \times A$ satisfying

$$x + \sqrt{D}y = (a + \sqrt{D}b)(c + \sqrt{D}d),$$

also (x, y) is a solution. Therefore we can state the following result:

Proposition 10.10. *If D is a plant and the set $Pell(D)$ contains one non-trivial solution, then it contains infinite many of them.*

Solutions to Pell's equation are related to automorphs, for we have the following result:

Proposition 10.11. *Suppose we are given a plant discriminant D and a form f with that discriminant. There is a one-to-one correspondence between $Aut(f)$ and $Pell(D)$.*

Proof. The proof is exactly identical to the one we did in $\mathbb{Z}$

□

Similarly, the μ-Pell's equation is related to another kind of transformation:

Proposition 10.12. *Suppose we are given a discriminant D and any form f with that discriminant. There is a one-to-one correspondence between μ-morphs of f and $\mu Pell(D)$.*

Proof. If we have $(a, b, c) \sim (\mu a, b, \frac{1}{\mu}c)$, then if the principal root of the first one is ω, the one of the second is $\frac{1}{\mu}\omega$. The rest follows exactly the same way we did in $\mathbb{Z}$.

□

Later we will try to take advantage of these bijections.

10.3 Half-reduced forms and class group

Far now, the plot we have followed coincides with the one we used for $\mathbb{Z}$. However, in the present case we will proceed faster with some alternative definitions.

Given a discriminant $D \in A$, we can partition all the forms with such discriminant into equivalence classes by means of the relation "$\sim$". We have the following definition:

Definition 10.13. *The set of equivalence classes under the relation "$\sim$" is called* the class group*, and it is denoted as $Cl(D)$.*

As we did in $\mathbb{Z}$, we will prove that it actually forms a group which we will call *the class group.*

Definition 10.14. *A form* (a, b, c) *is* half-reduced *if it satisfies*

$$|b| < |a| \leq |c|$$

The following two results will show the usefulness of this definition.

Proposition 10.15. *Given* D*, every class of* $Cl(D)$ *contains one half-reduced form.*

Proof. Suppose we are given a not half-reduced form (a, b, c) and an equivalent half-reduced form will be found.

In case $a = c = 0$, then it must be $b = \pm 1$, from the primitiveness. So, firstly, we apply S_1 and start from the form $(0, \pm 1, \pm 1)$. Therefore, we may assume a and c are not both zero.

We write $f_0 := (a, b, c)$ and follow this algorithm:

From the initial assumption, either a or c is not zero. Without loss of generality we suppose $a \neq 0$ (we could apply the transformation T). Then, we consider the unique $k \in A$ so that $|b + 2ak| < |a|$, which exists by means of the euclidean division. Note that k may be zero. We apply the transformation S_k to f_0 and get the form $(a, b + 2ak, ak^2 + bk + c)$.

If $|a| \leq |ak^2 + bk + c|$, this form is reduced and we are done. Otherwise, we apply T and define $f_1 := (a_1, b_1, c_1) = (ak^2 + bk + c, -b - 2ak, a)$. A new iteration starts with f_1.

Since $|b_1| < |b|$, i.e. the sequence of center coefficients is decreasing, the algorithm will eventually finish after $\deg b$ steps at most, finding a half-reduced form (A, B, C) equivalent to the given one.

□

Proposition 10.16. *Let* $D \in A$*. The set* $Cl(D)$ *is finite.*

Proof. Attending to last result, it is enough to show that the number of half-reduced forms is finite.

If we have $b^2 - 4ac = D$ where $|b| < |a| \leq |c|$, we must have $|a||c| = |D|$.

Therefore, if we write $\deg D = m$, the number of pairs $a, c \in A$ is at most

$$\sum_{k=0}^{k\leq m/2} q^{k+1}q^{m-k+1} \leq \frac{m+2}{2}q^{m+2}.$$

Once we determine a and c, there are at most 2 possible b so that $b^2 = D+4ac$. This means there are at most $(m+2)q^{m+2}$ half-reduced forms with such discriminant, which finishes the proof.

□

We are going to expose the theory of reduction of forms. Given a form f whose reduced equivalent form we aim to find, the first step will be finding one equivalent half-reduced form $f_{hr} = (a, b, c)$. We know it is possible to apply a transformation U_ψ to f_{hr} so that $\operatorname{sgn} a \in \{1, \mu\}$, where μ is a fixed non square of ${\mathbb{F}_q}^*$. This fact will be used almost in every proposition, for we will force all reduced forms to satisfy $\operatorname{sgn} a \in \{1, \mu\}$. Although we do it just for the sake of uniqueness, it will lead us to tricky situations, as we will see.

Chapter 11

Imaginary case

Definition 11.1. *A form (a, b, c) with odd discriminant D is* reduced *if*

$$|b| < |a| < |c| \text{ and } \operatorname{sgn} a \in \{1, \mu\}.$$

From now on we will implicitly assume that the determinants of all forms we will consider in this chapter have have odd degree.

Proposition 11.2. *Every class in $Cl(D)$ contains at least one reduced form.*

Proof. Given any form $f = (a, b, c)$, we know there exists an equivalent half-reduced form (A, B, C) such that $|B| < |A| \leq |C|$. This implies

$$\deg D = \deg \{B^2 - 4AC\} = \deg AC = \deg A + \deg C.$$

Since $\deg D$ is odd, the inequality is strict, hence $|B| < |A| < |C|$. We apply the adequate transformation U_ψ to make $\operatorname{sgn} A \in \{1, \mu\}$, and we are done.

□

We proved the existence, now we will go for the uniqueness with these two results:

Proposition 11.3. *If $f = (a, b, c)$ is reduced and $f' = (a', b', c')$, not necessarily reduced, is equivalent to f, then $|a| \leq |a'|$. If $|a| = |a'|$, then $a = a'$.*

Proof. First we note that a, c, a', c' cannot be zero for the opposite would imply that $\deg D$ is even. Since f and f' are equivalent, f represents a', hence we can write $f(X, Y) = a'$ for some $X, Y \in A$ (actually $(X, Y) =$

(α, γ), but this is unnecessary now). Completing the square as we did in equation 10.1, we deduce

$$4aa' = (2aX + bY)^2 - DY^2.$$

Since $\deg D$ is odd, the two summands in the right hand side of the equation have different degree. Therefore three options arise:

- $|aa'| = |DY^2|$, which implies $Y \neq 0$. Using that f is reduced we get

  $$|aa'| = |DY^2| = |a||c||Y|^2 > |a|^2|Y|^2,$$

  therefore $|a| < |a'|$, as desired. The equality is impossible in this case.

- $|aa'| > |DY^2|$ and $Y \neq 0$. Using f is reduced we have

  $$|a^2| < |a||c|Y^2 = |D||Y|^2 < |a||a'|,$$

  therefore $|a| < |a'|$, as desired. The equality is impossible in this case.

- $Y = 0$, hence $X \neq 0$. This implies $a' = aX^2$, therefore $|a| \leq |a'|$, as desired. If $|a| = |a'|$, then $X \in \mathbb{F}_q{}^*$. Since $\operatorname{sgn} a, \operatorname{sgn} a' \in \{1, \mu\}$, we deduce $a = a'$, as desired.

□

Proposition 11.4. *If $f = (a, b, c)$, where $|a| < |c|$, and $f' = (a', b', c')$, where $|a'| < |c'|$, are reduced and equivalent, then they are identical.*

Proof. Using last proposition, we have $|a| \leq |a'|$ and $|a'| \leq |a|$, therefore $|a| = |a'|$, which implies $a = a'$. From the equivalence equations 10.2 we get

$$0 = a(\alpha^2 - 1) + b\alpha\gamma + c\gamma^2$$

for a transformation $\alpha, \beta, \gamma, \delta \in A$ of the usual kind. Two options arise:

- If $\gamma \neq 0$, then, since $\deg a$ and $\deg c$ have different parity, also $\deg a(\alpha^2 - 1)$ and $\deg c\gamma^2$ have different parity. Combining this with the fact that f is reduced, implies

  $0 = \deg 0 = \deg\{a(\alpha^2 - 1) + b\alpha\gamma + c\gamma^2\} = \deg\{a(\alpha^2 - 1) + c\gamma^2\} =$

  $= \max[\deg\{a(\alpha^2 - 1)\}, \deg\{c\gamma^2\}] \neq 0,$

  which is an absurd.

- If $\gamma = 0$, then we must have $\alpha = \delta = \pm 1$. Therefore the transformation considered has the form S_β. But the second equivalence equation gives

$$b' = b + 2a\beta,$$

and, since $|b| < |a|$, the only β that can make $|b'| < |a|$ is $\beta = 0$. All in all, the transformation must be the identity, which finishes the proof.

□

All in all, along this chapter we have proved that the defined reduced forms are canonical representatives of the class group for the imaginary case.

Chapter 12

Pseudo-imaginary case

Definition 12.1. *A form* (a, b, c) *with even* $\deg D$ *and* $\operatorname{sgn} D \notin {\mathbb{F}_q}^{*2}$ *is* reduced *if*

$$|b| < |a| \leq |c| \text{ and } \operatorname{sgn} a \in \{1, \mu\}.$$

From now on we will implicitly assume that the determinants of all forms we will consider in this chapter have have even degree and $\operatorname{sgn} D \notin {\mathbb{F}_q}^{*2}$.

Since in this case the definition of reduced form and half-reduced form coincide, we can assert that every class in $Cl(D)$ contains at least one reduced form. For the uniqueness, we will have to distinguish the cases $|a| < |c|$ and $|a| = |c|$. First we study the case $|a| < |c|$.

Proposition 12.2. *If* $f = (a, b, c)$ *is reduced, where* $|a| < |c|$*, and* $f' = (a', b', c')$ *is equivalent to* f*, then* $|a| \leq |a'|$*. If* $|a| = |a'|$*, then* $a = a'$*.*

Proof. Firstly, we cannot have $a = 0$ since f is reduced. Now we can suppose $a \neq 0$, hence $c \neq 0$. Since f and f' are equivalent, f represents a', thus we can write $f(X, Y) = a'$ for some $X, Y \in A$. We have

$$4aa' = (2aX + bY)^2 - DY^2.$$

We note that $\operatorname{sgn}(2aX + bY)^2 \in {\mathbb{F}_q}^{*2}$ and, from the hypothesis, $\operatorname{sgn}\{-DY^2\} \notin {\mathbb{F}_q}^{*2}$, therefore the degree of the sum in the right hand side of the equation is the maximum degree of the summands. From this point, the demonstration exactly coincides with the one we did for proposition 11.3

□

Proposition 12.3. *If* $f = (a, b, c)$*, where* $|a| < |c|$*, and* $f' = (a', b', c')$*, where* $|a'| < |c'|$*, are reduced and equivalent, then they are identical.*

Proof. We repeat the strategy of proposition 11.4. From last proposition, $a = a'$. The first equivalence equation has the form

$$0 = a(\alpha^2 - 1) + b\alpha\gamma + c\gamma^2$$

for a transformation $\alpha, \beta, \gamma, \delta \in A$ of the ususal kind. Two options arise:

- $\gamma \neq 0$: If we had $\operatorname{sgn} c = -\psi^2 \operatorname{sgn} a$ for some $\psi \in {\mathbb{F}_q}^*$, since f is reduced, it would imply

  $$\operatorname{sgn} D = \operatorname{sgn}\{b^2 - 4ac\} = \operatorname{sgn}\{-4ac\} = (2\psi \operatorname{sgn} a)^2,$$

  which would be an absurd. Therefore, $\operatorname{sgn}\{a(\alpha^2 - 1) + c\gamma^2\} \neq 0$, and the first equivalence equation cannot hold.

- If $\gamma = 0$, then $\alpha = \delta = \pm 1$. The transformation has the form S_β. The second equivalence equation gives $b' = b + 2a\beta$, and, since $|b| < |a|$, the only β that can make $|b'| < |a|$ is $\beta = 0$, so f and f' are identical.

□

So we have deduced that the mentioned kind of reduced forms are unique in its equivalence class. Thus a reduced form with $|a| = |c|$ could just be equivalent to another form of this kind. We have the following result:

Proposition 12.4. *Let $f = (a, b, c)$ be reduced, where $|a| = |c|$. Consider the following two kinds of forms:*

- $f|_T$
- $f|_{TS_{p_1}T}$, *where* $p_1 \in {\mathbb{F}_q}^*$

Each of these forms can be reduced, in the first case applying an adequate transformation U_γ, in the second one applying adequate S_{p_2} and U_{p_3}. All and only those reduced forms belong to the equivalence class of f.

Proof. Let $f' = (a', b', c')$ be a reduced form, where $|a'| = |c'|$, so that $f \sim f'$. Since f and f' are reduced, a, c, a', c' cannot be zero. Without loss

of generality, we can suppose $|a'| \leq |a|$. Now, f and f' are equivalent, so there exists a transformation M of the usual kind so that

$$f(\alpha,\gamma)X^2 + [b(\alpha\delta+\beta\gamma)+2(a\alpha\beta+c\gamma\delta)]XY + f(\beta,\delta)Y^2 = f'(X,Y).$$

Therefore $f(\alpha,\gamma) = a'$. We have

$$4aa' = (2a\alpha+b\gamma)^2 - D\gamma^2.$$

Again, the degree of the sum in the right hand side of the equation is the maximum degree of the summands. We act like we did in proposition 11.3, the options are:

- $|aa'| > |D\gamma^2|$ and $\gamma \neq 0$. Using f is reduced we have

  $$|a^2| \leq |a||c||\gamma|^2 = |D||\gamma|^2 < |a||a'|,$$

  therefore $|a| < |a'|$, which is an absurd.

- $\gamma = 0$, which implies $\alpha = \delta = \pm 1$. So $a = a'$, and the transformation has the form S_β. As we did in last proposition, we deduce that $\beta = 0$, so the transformation is actually the identity.

- $|aa'| = |D\gamma^2|$, so $\gamma \neq 0$. This means we have $|a'| = |a||\gamma|^2$. Since $|a'| \leq |a|$, we must have $\gamma \in {\mathbb{F}_q}^*$ and $|a| = |a'|$. But $a' = f(\alpha,\gamma)$ and therefore

  $$|a'| = |a\alpha^2 + c\gamma^2|.$$

  Combined with $|a'| = |a| = |c|$, this means $|\gamma| \geq |\alpha|$, i.e. that $\alpha \in \mathbb{F}_q$. We must distinguish two cases now, $\alpha = 0$ and $\alpha \neq 0$.

  If $\alpha = 0$, then

  $$M = \begin{pmatrix} 0 & -\gamma^{-1} \\ \gamma & \delta \end{pmatrix},$$

  and $b' = -b + 2c\gamma\delta$, whose degree is less than $\deg c$ only if $\delta = 0$. Our transformation becomes $M = TU_\gamma$, so $(a', b', c') = (c\gamma^2, -b, a\gamma^{-2})$, obviously reducible. It is left to determine the coefficient γ, but it follows from $\operatorname{sgn} c\gamma^2 \in \{1, \mu\}$. Therefore f' is the form $f|_T$ where the first term has been normalized.

  If $\alpha \neq 0$, then we have the identity

  $$M = \begin{pmatrix} \alpha & 0 \\ \gamma & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1 & \beta/\alpha \\ 0 & 1 \end{pmatrix} = S^T_{\gamma/\alpha} U_\alpha S_{\beta/\alpha} = T S_{\gamma/\alpha} T S_{\alpha\beta} U_\alpha.$$

  We can define $p_1 := \gamma/\alpha; \quad p_2 := \alpha; \quad p_3 := \beta/\alpha$ to write M as

  $$M = T S_{p_1} T S_{p_2} U_{p_3}.$$

So let's examine the way M acts, assuming f' is reduced.

Every $p_1 \in \mathbb{F}_q{}^*$ defines a different form $f|_{TS_{p_1}T} = (a + bp_1 + cp_1{}^2, b + 2cp_1, c)$, obviously reducible. The only possible option is that the transformation S_{p_2} normalizes the center term, which uniquely determines S_{p_2}, and then U_{p_3} normalizes the right term, which uniquely determines U_{p_3}. This finishes the proof.

□

Chapter 13

Real case

Definition 13.1. *A form (a, b, c) whose discriminant D is a plant is* reduced *if*

$$|\sqrt{D} - b| < |a| < |\sqrt{D}|.$$

The absence of $\operatorname{sgn} a \in \{1, \mu\}$ is specially remarkable. We prefer to forget this condition through this chapter, for it will make more explicit some properties of the cycles of reduced forms. Later we will introduce it in order to have an uniform type of reduced forms in all chapters.

We recall that we say D is a plant if D is not a perfect square, $\deg D$ is even and $\operatorname{sgn} D \in {\mathbb{F}_q}^{*2}$. It was proved in the preamble that plants and perfect squares are the only elements in R whose square root exists in R. If $\operatorname{sgn} D = \rho^2$, then we can choose $\sqrt{D}$ to have $\operatorname{sgn} \sqrt{D} = \rho$ or $\operatorname{sgn} \sqrt{D} = -\rho$. When we write $\sqrt{D}$ we will be refering to the one with ρ sign. Plus, we will implicitly assume that all forms in this chapter have plant discriminant.

The inequality $|\sqrt{D} - b| < |\sqrt{D}|$ implies $|b| = |\sqrt{D}|$ and $\operatorname{sgn} b = \operatorname{sgn} \sqrt{D}$, so we can write this inequality imitating the one we used for the case in $\mathbb{Z}$ as $|\sqrt{D} - b| < |2a| < |\sqrt{D} + b|$. Many more similarities will arise along this chapter.

In the imaginary and pseudo-imaginary cases it was not necessary to prove the finiteness of the defined reduced forms, for the reduced forms are almost unique in their equivalence classes. In this case it is more convenient to state this result now:

Proposition 13.2. *Given a plant $D \in A$, there is a finite number of reduced forms with such discriminant.*

Proof. Since $|\sqrt{D} - b| < |\sqrt{D}|$ implies $|b| = |\sqrt{D}|$, we have

$$0 < |a| < |b| = |D|,$$

where we noted that a cannot be zero for D would be a square. Therefore, given D, roughly speaking there are at most $|D|$ possible b's and $|D|$ possible a's, hence $|D|^2$ possible pairs. Since c is determined when these two are chosen, there are at most $|D|^2$ reduced forms with the given discriminant, which finishes the proof.

□

Lemma 13.3. *Any form $f = (a, b, c)$ satisfies*

$$|\sqrt{D} - b| < |a| < |\sqrt{D}| \iff |\sqrt{D} - b| < |c| < |\sqrt{D}|.$$

Proof. It is enough to prove $\Rightarrow$, for the other one follows by symmetry.

Since $D = b^2 - 4ac$, we have $|\sqrt{D} - b||\sqrt{D} + b| = |a||c|$. But, as we said, $|\sqrt{D} + b| = |b|$, hence we can rewrite it as

$$|\sqrt{D} - b||\sqrt{D}| = |a||c|.$$

If, for instance, we had $|c| \leq |\sqrt{D} - b|$, it would imply

$$|\sqrt{D} - b||\sqrt{D}| = |a||c| < |\sqrt{D}||\sqrt{D} - b|,$$

which is an absurd. We act analogously with $|c| \geq |\sqrt{D}|$ and we are done.

□

Attending to this equivalence, from now on we will conveniently use one inequality or the other when considering reduced forms.

Proposition 13.4. *Every class in $Cl(D)$ contains at least one reduced form.*

Proof. Since every class in $Cl(D)$ contains one half-reduced form, it is enough to show that they have an equivalent reduced form. Let g be a half-reduced form. We apply T to g and get a form $f_0 = (a_0, b_0, a_1)$ so that

$$|b_0| < |a_1| \leq |a_0|.$$

This implies $|b_0| < |\sqrt{D}|$ and $|a_1| \leq |\sqrt{D}|$.

We consider the form $f_1 = (a_1, b_1, a_2)$, which we will force to be right adjacent to f_0. To that end, it is enough to choose $b_1 = -b_0 + 2a_1k$ for any

$k \in A$ and $a_2 = \frac{b_1^2 - D}{4a_1}$ However, since $|a_1| \leq |\sqrt{D}|$ and $|\sqrt{D} + b_0| = |\sqrt{D}|$, there exists one unique $k \in A$ so that

$$|\sqrt{D} - b_1| = |(\sqrt{D} + b_0) - 2a_1 k| < |a_1| \leq |\sqrt{D}| = |\sqrt{D} - b_0|.$$

Such a k can be obtained from the euclidean division of $\lfloor \sqrt{D} \rfloor + b_0$ over $2a_1$ or we could simply set $k = \lfloor \frac{b_0}{a_1} \rfloor$, but it is unnecessary for our purposes. Anyway, this k is unique and we write $b_1 = -b_0 + 2a_1 k$. Since it satisfies $|\sqrt{D} - b_1| < |\sqrt{D}|$, we have $|\sqrt{D}| = |b_1|$.

As a consequence of this construction, also the following inequality holds:

$$|a_2| = \frac{|b_1 + \sqrt{D}||b_1 - \sqrt{D}|}{|a_1|} = \frac{|b_1||b_1 - \sqrt{D}|}{|a_1|} < \frac{|\sqrt{D}||a_1|}{|a_1|} = |\sqrt{D}|$$

If $|a_2| > |\sqrt{D} - b_1|$ we are done since f_1 . Otherwise, it must be $|a_2| \leq |\sqrt{D} - b_1|$, so we consider the form $f_2 = (a_2, b_2, a_3)$, which we will force to be right adjacent to f_2, as we did before. We set $b_2 = -b_1 + 2a_2 k$, and since $|a_2| \leq |\sqrt{D} - b_1|$, there exists at least one k so that

$$|\sqrt{D} - b_2| = |\sqrt{D} + b_1 - 2a_1 k| < |\sqrt{D} - b_1|.$$

The pattern is clear now. It we apply this algorithm repeatedly with f_i, it must eventually come up with a reduced form , for otherwise we would get an infinite decreasing sequence $(|\sqrt{D} - b_i|)_{i \in \mathbb{N}_0}$. Note that, since $b_i \in A$, the inequality $|\sqrt{D} - b_i| \geq \frac{1}{q}$ holds for every $i \in \mathbb{N}_0$.

□

In the two previous chapters, when we arrived to this point we aimed to prove the uniqueness of the reduced forms in their respective classes. As it happened in the indefinite case in $\mathbb{Z}$, adjacency will play a main role in this purpose, starting from the following result:

Proposition 13.5. *Every reduced form has an unique reduced adjacent form to the right and to the left.*

Proof. It is enough to prove it for the right adjacency, the left case follows analogously.

Consider the reduced form $f = (a, b, c)$. If $f' = (c, b', c')$ is one of its right adjacent forms it must satisfy $b' = -b + 2ck$, where $k \in A$ and c' is determined by the discriminant. Therefore what we want to show is that one

and only one k can be chosen to make f' reduced . We want the following inequality to hold:

$$|\sqrt{D} + b - 2ck| < |c| < |\sqrt{D}|$$

However, since f is reduced, the inequality $|c| < |\sqrt{D}|$ is obviously satisfied. For the first one, we note that $|\sqrt{D}+b| = |\sqrt{D}| > |c|$ therefore the euclidean division (taking $\lfloor\sqrt{D}\rfloor$ instead of $\sqrt{D}$) gives the unique k which makes $|\sqrt{D} + b - 2ck| < |c|$, and we are done.

□

We need to explain how these forms can be arranged:

As we did in $\mathbb{Z}$, we can partition the set of reduced forms of a given discriminant into cycles of adjacent forms. We do not repeat all the details again for the process is identical. We choose any reduced form f and start a cycle moving forward to the next right adjacent form. Since the reduced forms with a fixed discriminant are finite, eventually we return to f without having repeated any other form before. If there are no reduced forms left, we are done. Otherwise, we choose a new form and repeat the process, until there are no reduced forms left.

Definition 13.6. *The number of reduced forms in a cycle is called the* period *of the cycle.*

Since adjacent forms are equivalent, these cycles are composed of equivalent forms. We would like to prove that if two forms are equivalent, then they belong to the same cycle. However, unlike the case in $\mathbb{Z}$, this result has many nuances.

13.1 Behavior of the cycles

Our efforts into finding an invariant such as the sign alternation for the cycles in $\mathbb{Z}$ were vain, so we were not able to prove that all cycles have even period. We started to suspect that the existence of such a proof was an illusion when we discovered the cycles of length 1, compounded by a form of the following type:

$$(\psi, b, \psi), \text{ provided } \psi \in (\mathbb{F}_q)^*,\ b \in A \text{ and } \lfloor\sqrt{b^2 - 4\psi^2}\rfloor = b.$$

We invite the reader to check there are many non-trivial, easy-to-check polynomials satisfying last property, such as $b = T^n$. We shall call a cycle of this kind *a trivial cycle*. Although we have not found any of them explicitly, we

will carry on the possibility of non-trivial cycles with odd period, for it is beautiful enough to deserve existence.

Definition 13.7. *We will refer to a form which is its own associate, i.e. to a form of the type* (a, b, a)*, not necessarily ambiguous, as a* selfie.

Definition 13.8. *If a form is either ambiguous or a selfie, we will call it a* rare *form.*

Therefore the mentioned form (ψ, b, ψ) is both a selfie and ambiguous, which is impossible in the definite case in $\mathbb{Z}$. This example informs us about the existence of some details in this part of our work that we should not overlook, so it is necessary to be extremely careful along the following demonstrations.

We suppose the associated forms f and f' are in different cycles. Then moving towards the right adjacent form of f we will get the associated form of the one we get moving towards the left adjacent form of f', and so on if we continue the process. Thus, we call these cycles *associated*.

Analogously, if the associated forms f, f', different or not, are in the same cycle, then this process associates the cycle with itself, so we will say the cycle is *self-associated*.

Definition 13.9. *Given a reduced form* f_1*, if the forms we successively get when cycling forward (i.e. to the right adjacent form) in the cycle are* $f_2, f_3 \cdots$ *then we define* the distance from f_1 to f' *as* $k-1$*, where* k *is the minimum natural number such that* $f' = f_k$*. We will also write it as* $dist(f_1, f')$*.*

Now we will repeatedly use the fact, easy to prove and already mentioned, that an ambiguous form is right adjacent to its associate, and conversely that a pair of associated adjacent forms must be an ambiguous form and its associate.

Proposition 13.10. *Suppose we are given a cycle with even period. If it contains one rare form, then it contains exactly two rare forms, which are either both selfies or both ambiguous, and the cycle is self-associated.*

Conversely, if a cycle with even period is self-associated, it contains exactly two rare forms, and they are either both selfies or both ambiguous.

In both cases, the distance from one rare form to the other one is half the period of the cycle.

Proof. ($\Rightarrow$) First we suppose the cycle contains the ambiguous form (a, ak, c), where $k \in A$. Its associate (c, ak, a) is also its right adjacent form. Note that they cannot be the same form. We cycle forward from (c, ak, a) and backwards from (a, ak, c), getting successively pairs of associated forms. Since the cycle is finite and has even period, we finish the process when we arrive to a pair of different forms which are adjacent and associated.

Therefore, the form we got cycling from (c, ak, a) is the other ambiguous form (it could be the form (c, ak, a) itself), and attending to the way the pairs of associated forms were distributed, the two ambiguous forms we have mentioned are the only two possible ones. From the process we have followed, we also deduce that the given cycle is its own associate and also that the distance from (a, ak, c) until the other ambiguous is half the period.

Now we suppose the cycle contains the selfie (a, b, a). We cycle forward and backwards from (a, b, a), getting successively pairs of associated forms. Since the cycle is finite and has even period, we finish the process when we arrive to a selfie.

From the way the pairs of associated forms were distributed, these two selfies are the only two possible ones. From the process we have followed, we also deduce that the given cycle is self-associated and also that the distance from one rare form to the other one is half the period.

($\Leftarrow$) We assume the given cycle is self-associated. If **every** form is a selfie, then the period must be 2 and the cycle is $(a, b, a) \sim (a - b, a)$, which agrees with the statement.

Otherwise we choose two different associated forms f, f' in the cycle and cycle forward from f and backwards from f' through pairs of associated forms, so we are moving just in one arc of the cycle. We have two options:

- If $dist(f, f')$ is even, then eventually we come up with a selfie. Since $dist(f', f)$ is also even, then we do the same process cycling along the other arc of the cycle and we find the second selfie. The cycle cannot contain more since following this process we checked all the forms in it.

- If $dist(f, f')$ is odd, then we arrive to two adjacent associated forms $(a', b, a) \sim (a, b, a')$ (maybe f', f themselves, respectively). This implies (a, b, a') is ambiguous. Since $dist(f', f)$ is also odd, using the other arc of the cycle, we repeat the process and get a different ambiguous form, so we have two of them. The cycle cannot contain more, from the followed process.

□

Example Working in $\mathbb{F}_3$, we fix $D = T^4 + 1$. One of its cycles is the self-associated one:

$$(2T, T^2 + 1, T) \sim (T, T^2 + 2, T) \sim (T, T^2 + 1, 2T) \sim (2T, T^2 + 2, 2T)$$

Indeed, it contains two rare forms, in particular two selfies.

Proposition 13.11. *Suppose we are given a cycle with odd period. If it contains one rare form, then it contains exactly two rare forms, which are one selfie and one ambiguous form, and the cycle is self-associated.*

Conversely, if a cycle with odd period is self-associated, it contains exactly two rare forms, and they are one selfie and one ambiguous form.

In both cases, if the ambiguous form is f_a, the selfie is f_s and the period is $2m + 1$, then $dist(f_a, f_s) = m + 1$.

Proof. ($\Rightarrow$) If the cycle contains the ambiguous form f_a, then its associate f'_a is also its right adjacent form. If they are the same form, the cycle is trivial (note that the trivial case contains exactly one selfie and one ambiguous form).

Otherwise we cycle forward from f'_a and backwards from f_a, getting successively pairs of associated forms. Since the cycle is finite and has odd period, we finish the process when we arrive to a selfie f_s. Since $dist(f'_a, f_s) = m$, we have $dist(f_a, f_s) = m + 1$.

Attending to the way the pairs of associated forms were distributed, there are no more rare forms. Also, the cycle is self-associated.

On the other hand, if the cycle contains the selfie f_s, then again we cycle forward and backwards from f_s, getting successively pairs of associated forms. Since the cycle has odd period, we finish the process when we arrive to a pair of adjacent, associated forms, i.e. we have found the ambiguous form f_a. The rest follows similarly as in the previous case.

($\Leftarrow$) We assume the given cycle is its own associate. If **every** form is a selfie, then the period must be 1 and we are dealing with the trivial case. Otherwise we choose two different associated forms f, f' and we can suppose $dist(f, f')$ is even and $dist(f, f')$ is odd. We start moving in the cycle, forward from f and backwards from f', through pairs of associated

forms. Finally this pair coincides in an unique form, so we have found a selfie. Considering the other arc, we find the ambiguous form.

□

The most relevant self-associated cycle is *the principal cycle*. It cannot be defined as the one containing the principal form I_D, for it is not reduced, so we define it as the one containing the *principal reduced form* of discriminant D, defined as

$$I_p := (1, b, c) \text{ where } b = \lfloor \sqrt{D} \rfloor \text{ and } c = \frac{\lfloor \sqrt{D} \rfloor^2 - D}{4}.$$

It is easy to prove that I_p is actually reduced. Its principal root is

$$\omega_p := \frac{-\lfloor \sqrt{D} \rfloor + \sqrt{D}}{2}.$$

The principal reduced form $I_p = (1, b, c)$ is equivalent to $I_D = (1, 0, \frac{-D}{4})$, for they share discriminant.

13.2 Cycles and continued fractions

As we may have guessed, the cycle of a reduced form and the simple continued fraction (scf) of its principal root are closely related.

We consider a reduced form (a, b, a') and its right adjacent reduced form, (a', b', a''). We define $\delta := -\frac{b+b'}{2a'}$ and, as we know, these two forms are properly equivalent via the transformation

$$N_\delta = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}.$$

It is important to note that, from the definition of reduced form, the polynomial δ cannot be constant. If ω and ω' are the two principal roots of the forms considered, we know the following equation holds

$$\omega = \frac{1}{\delta - \omega'}.$$

We repeat the process: assuming the form (a', b', a'') becomes its right adjacent one via the transformation $\begin{pmatrix} 0 & 1 \\ -1 & \delta' \end{pmatrix}$, we get $\omega' = \frac{1}{\delta' - \omega''}$, therefore

$$\omega = \frac{1}{\delta + \frac{1}{-\delta' + \omega''}}.$$

We easily deduce how to continue: given a cycle of period m, let's say $f_1, \cdots, f_m$ are the forms which compound the cycle. Assuming $\begin{pmatrix} 0 & 1 \\ -1 & \delta_k \end{pmatrix}$ is the transformation which converts f_k into f_{k+1} and ω_k is the principal root of f_k, then for any $k \in [m]$ the following scf expansion holds

$$\omega_k = [0; *\delta_k, -\delta_{k+1} \cdots, (-1)^{m-1}\delta_{k+m-1}, (-1)^m \delta_k, \cdots, *\delta_{k+m-1}],$$

where we implicitly assume that if $k + m - 1 > m$ then we must take $k - 1$ instead.

Proposition 13.12. *The scf of $\omega \in A$ is periodic iff ω is an irrational root of a quadratic equation with coefficients in A.*

Proof. ($\Rightarrow$) This case is identical to the one in $\mathbb{Z}$. Let $\omega = [a_0; \cdots, *a_I, \cdots, *a_{I+p-1}]$ and $X_I = [*a_I; \cdots, *a_{I+p-1}]$. If P'/Q' and P''/Q'' are the last two convergents of $[a_I; \cdots, a_{I+p-1}]$ then, since $X_I = [a_I; \cdots, a_{I+p-1}, X_I]$, we must have

$$X_I = \frac{P'X_I + P''}{Q'X_I + Q''},$$

so X_I is a quadratic irrational (we know it is irrational for otherwise its scf would be finite). Since $\omega = [a_0; \cdots, a_{I-1}, X_I]$, using the last two convergents of $[a_0; a_1, \cdots a_{I-1}]$, ω has the form

$$\omega = \frac{P_{I-1}X_I + P_{I-2}}{Q_{I-1}X_I + Q_{I-2}}.$$

Since ω is a rational function of a quadratic irrational, it is also a quadratic irrational, as desired.

($\Leftarrow$) First of all we should not miss a relevant fact: the field R contains only the square roots of plants and squares, and no other kind of polynomials.

Thus let's suppose $a\omega^2 + b\omega + c = 0$, where $a, b, c \in A$ are coprime. We have $\omega = \frac{-b+\sqrt{D}}{2a}$, therefore the existence of ω, which is our hypothesis, implies the existence of $\sqrt{D}$. In other words, $\deg D$ is even and $\operatorname{sgn}(D) \in \mathbb{F}_q^{*2}$, which means that we are in the "real case".

We consider the form $f = (a, b, c)$, not necessarily reduced. Multiplying f by -1 if needed, we assume that ω is the principal root of f. There exists at least one reduced form $F = (A, B, C)$ so that $f \sim F$. Let Ω be the principal root of F. Since these two forms are equivalent, there exist $\alpha, \beta, \gamma, \delta \in A$ so that $\alpha\delta - \beta\gamma = 1$ and

$$\omega = \frac{\alpha\Omega + \beta}{\gamma\Omega + \delta}.$$

If $\Omega = [0; *r_1, \cdots, *r_p]$, where p is minimum, then we apply corollary 9.22 and get

$$\omega = \pm\psi^2[a_0; \cdots, a_M, *r_1, \cdots, *r_p],$$

for some $a_0 \cdots a_M \in A$ which are not constant. It is easy to see that this finishes the proof.

□

Proposition 13.13. *The scf of $\omega \in A$ is pure periodic iff it is the principal root of a reduced form.*

Proof. ($\Leftarrow$) It follows from the equivalence between moving in the cycle and developing the scf. Again we should note that, if ω is the principal root of a reduced form, then that form belongs to the "real case".

($\Rightarrow$) Suppose ω has a pure periodic scf $[0; *a_1, \cdots, *a_{p_1}]$, where p_1 is minimum. Since it is periodic, we know there exist essentially unique coprime $a, b, c \in A$ such that

$$a\omega^2 + b\omega + c = 0,$$

where we can suppose ω is the principal root of the form $f = (a, b, c)$. As we did before, there exists a reduced form $F = (A, B, C) \sim f$. So using corollary 9.22, if $\Omega = [0; *r_1, \cdots, *r_{p_2}]$, where p_2 is minimum, we can write

$$\omega = \pm\psi^2[t_0; \cdots, t_M, *r_1, \cdots, *r_{p_2}],$$

where last expression is a scf. This $\pm\psi^2 \in \mathbb{F}_q^*$ is a not a big problem in the following reasonings, where we will omit it for the sake of clearance (we can imagine we have introduced it into the scf although we maintain the name of all quotients and the period, which may have changed).

Since every scf is unique, from

$$[0; *a_1, \cdots, *a_{p_1}] = [t_0; \cdots, t_M, *r_1, \cdots, *r_{p_2}]$$

we deduce that all quotients are identical, which means the period of Ω must be a cyclical permutation of that of ω. Therefore if we move to the right adjacent form starting from F, eventually we come up with a form f' satisfying that, if ω' is its principal root, then

$$\omega' = \pm\psi^{\pm 2}\omega,$$

where both $\pm$ signs are independent. In any case, since the principal root completely determines a form whose discriminant is known, some of these forms is reduced:

$$(\pm a\psi^{\pm 2}, b, \pm c\psi^{\mp 2}),$$

where the dependent signs are $(\pm a)(\pm c) = ac$ and $\psi^{\pm 2}\psi^{\mp 2} = 1$. This implies $f = (a, b, c)$ is reduced, as desired.

□

As we did in $\mathbb{Z}$, we would like to sharpen our knowledge of the optimal period of the principal root of a form as a function of the period of the cycle where it is contained. Far now, all we know is that the period of the principal root is a divisor of double the period of the cycle. For the following proposition, we will follow the notation we have used along this section: given a cycle of period m, we say $f_1, \cdots, f_m$ are the forms which compound the cycle. The matrix $\begin{pmatrix} 0 & 1 \\ -1 & \delta_k \end{pmatrix}$ is the transformation which converts f_k into f_{k+1} and ω_k is the principal root of f_k, hence the following scf expansion holds

$$\omega_1 = [0; *\delta_1, -\delta_2 \cdots, (-1)^{m-1}\delta_m, (-1)^m\delta_1, \cdots, *(-1)^{2m}\delta_m].$$

Suppose also that the optimal period of ω_1 is p.

Proposition 13.14. *If m is even, then $p = m$. If m is odd, $p = 2m$.*

Proof. Suppose m is even. Then p must divide m. In general the following equation holds

$$\omega_1 = [0; \delta_1, -\delta_2 \cdots, (-1)^{p-1}\delta_p, \frac{(-1)^p}{\omega_{p+1}}].$$

However, from the hypothesis we also have

$$\omega_1 = [0; \delta_1, -\delta_2 \cdots, (-1)^{p-1}\delta_p, \frac{(-1)^p}{\omega_1}].$$

We isolate ω_1 and ω_{p+1}, arriving to $\omega_1 = \omega_{p+1}$. Since the principal root completely determined the form, this means $f_1 = f_{p+1}$, so we must have $p = m$, as desired.

For the case where m is odd, p must divide $2m$, so suppose first that $p \leq m$. Repeating the last reasoning we would arrive to $p = m$. However this contradicts the scf expansion

$$\omega_1 = [0; *\delta_1, -\delta_2 \cdots, (-1)^{m-1}\delta_m, (-1)^m\delta_1, \cdots, *(-1)^{2m}\delta_m],$$

for it would imply that all coefficients are zero. Therefore $p = 2m$, as desired.

□

13.3 Equivalence and cycles

Now we will focus on showing in what sense equivalence implies sharing cycle. This case is much trickier than the one in $\mathbb{Z}$.

Definition 13.15. *The cyclically ordered set of forms that compound the cycle of f shall be referred as $Cic(f)$.*

Theorem 13.16. *If $f \sim f'$ and $f' = (a', b', c')$, then there exists $\psi \in \mathbb{F}_q^*$ such that $(a', b', c')|_{U_\psi} \in Cic(f)$ or $(-a', b', -c')|_{U_\psi} \in Cic(f)$.*

Proof. Suppose ω, ω' are the principal roots of f and f'. Since $f \sim f'$, there exists a properly equivalent transformation $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ making $f|_M = f'$, and therefore

$$\omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta},$$

so using corollary 9.22, if $\omega' = [0; *r_1, \cdots, *r_p]$, we can write

$$\omega = \pm\psi^2[a_0; \cdots, a_M, *r_1, \cdots, *r_p]$$

for some M and some $a_i \in A$ such that $|a_i| > 1$, i.e. it is a scf.

Since ω has a pure periodic scf, from their uniqueness we deduce that the period of ω must be a cyclical permutation of the period of ω', provided the constant $\pm\psi^2$ has been introduced into the scf. Therefore if we move to the right adjacent form starting from f, finally we find a form F satisfying that, if Ω is its principal root, then

$$\Omega = \pm\psi^{\pm 2}\omega',$$

for some choice of the signs, where both $\pm$ signs are independent. Since the principal root determines a form, we deduce

$$F = (\pm a'\psi^{\pm 2}, b', \pm c'\psi^{\mp 2}),$$

where the dependence between signs is $(\pm a)(\pm c) = ac$ and $\psi^{\pm 2}\psi^{\mp 2} = 1$. This finishes the proof.

□

This result is a bit disappointing compared to the one we got in $\mathbb{Z}$. However at least the square was unavoidable, as we would like to explain now.

First of all, recall that we have not forced our reduced forms to satisfy $\operatorname{sgn} a \in \{1, \mu\}$. Why increasing so unnecessarily the number of reduced forms? Because the condition $\operatorname{sgn} a \in \{1, \mu\}$ is, at least *a priori*, unnatural when studying cycles. It would provoke that, when moving forward from the form (a, b, c) through its "adjacent" forms (the definition would have to be different), many normalizing matrices were involved, and finally we would have messed up the simplicity of cycles in a sea of squared constants. It may work, actually, but we are still on time to consider this "class". Before doing so, there is a question which is specially interesting for us:

Is it possible that $f|_{U_\psi} \in Cic(f)$?

We think it is not possible. An example may help us understand.

Example In $\mathbb{F}_5$, if $D = T^4 + T + 1$, we consider $f = (3, T^2, 2T + 2)$. Its cycle is the following one:

$$(3, T^2, 2T+2) \sim (2T+2, T^2+3, 2T+1) \sim (2T+1, T^2+4, T) \sim (T, T^2+1, 3T+1) \sim$$

$$\sim (3T+1, T^2+1, T) \sim (T, T^2+4, 2T+1) \sim (2T+1, T^2+3, 2T+2) \sim (2T+2, T^2, 3)$$

It is easy to check that the adjacency $(a, b, c) \sim (c, d, e)$ implies the adjacency $(\psi a, b, \frac{1}{\psi} c) \sim (\frac{1}{\psi} c, d, \psi e)$ for every $\psi \in \mathbb{F}_q$. Therefore, the fact that the principal form $I_D = (1, T^2, T + 1)$ does not belong to this cycle implies that $Cic(I_D)$ is like $Cic(f)$ "multiplied" by a constant, and obviously disjoint. If instead of I_D we take

$$g = (2^2 \times 3, T^2, 2^{-2} \times (2T + 2)) = (-3, T^2, -(2T + 2)) = (2, T^2, 3T + 3),$$

so we see $g \sim f$ although they do not belong to the same cycle, and again, the difference between these two cycles is simply this constant factor. Note that $-1 = 2^2$ is a square.

As we can see through this example, theorem 13.16 is not as non-optimal as it seems. The squares are necessary, and the appearance of the negative sign is, if not necessary, at least not completely wrong. On the other hand, we have not been able to give a satisfactory answer to whether $f|_{U_\psi} \in Cic(f)$ is possible or not. We think a demonstration of this fact should be based on establishing an isomorphism between $Aut(f)$ and $Pell(D)$. However, we can manage without this proof.

Let a form $f_1 = (a, b, c)$ be considered. We start moving through its cycle, which has period m, passing by the forms $f_2, \cdots, f_m$, and finally $f_{m+1} = f_1$. We define l as the minimum natural number satisfying that there exists a constant $\chi \in (\mathbb{F}_q)^*$, square or not, such that $f_{l+1} = (\chi a, b, \frac{1}{\chi} c)$.

Since the adjacency $(a,b,c) \sim (c,d,e)$ implies the adjacency $(\chi a, b, \frac{1}{\chi}c) \sim (\frac{1}{\chi}c, d, \chi e)$, we have the following possibilities:

1. If $\chi = 1$, then $l = m$ and they can be odd or even. It is not possible that $f|_{U_\psi} \in Cic(f)$.
2. If $\chi \neq 1$ and l is odd, then $2l = m$. It can happen $f|_{U_\psi} \in Cic(f)$ depending on χ is a square or not.
3. If $\chi \neq 1$ and l is even, then the cycle has the form

$$(a,b,c) \sim \cdots \sim (\chi a, b, \frac{1}{\chi}c) \sim \cdots \sim (\chi^2 a, b, \frac{1}{\chi^2}c) \sim \cdots$$

and we deduce $m = ord(\chi)l$. It could happen $f|_{U_\psi} \in Cicf$.

Now it is the moment to consider the standard definition of reduced form. Although we will use a tedious notation, it is worth it in order to avoid misunderstandings.

Definition 13.17. *If $f|_{U_\psi} = g$, we will say $f \sim_U g$. This is an equivalence relation whose class will be denoted as $[f]_U$. The representative of this class is the only form $f = (a,b,c)$ such that* $\operatorname{sgn} a \in \{1, \mu\}$.

Two classes $[f]_U$ and $[g]_U$ are equivalent *if their representatives are equivalent, and we will write $[f]_U \sim [g]_U$.*

Two classes $[f]_U$ and $[g]_U$ are adjacent *if there exists $\psi \in \mathbb{F}_q$ such that $f|_{U_\psi}$ and g are adjacent.*

The third part is well defined since, as we have repeatedly said, the adjacency $f \sim g$ implies the adjacency $f|_{U_\psi} \sim g|_{U_{\psi^{-1}}}$. Cycles of forms $[f]_U$ can be understood as cycles of forms f which finish when we pass through any form of the type $f|_{U_\psi}$. Concretely, the three types of cycles we mentioned experience the following changes:

1. If $\chi = 1$, as before, then $l = m$ and they can be odd or even. However, what does change is that now all disjoint cycles which differed only by a product U_ψ now are identified. More exactly, $\frac{q-1}{2}$ cycles are identified.
2. If $\chi \neq 1$ and l is odd, there are two cases. The first one, if χ is a square, then actually $[f_{l+1}]_U = [f_1]_U$, so $l = m$ and we are in the case (1). If χ was not a square, we have $2l = m$. Again, cycles deferring by the product of a transformation U_ψ are identified.

3. If $\chi \neq 1$ and l is even, again we have two options. If χ is a square then again $[f_{l+1}]_U = [f_1]_U$ since $[(a,b,c)]_U = [(\chi a, b, \frac{1}{\chi}c)]_U$, hence $m = l$ and we are in case (1). Otherwise,

$$(a,b,c) \sim \cdots \sim (\chi a, b, \frac{1}{\chi}c) \sim \cdots \sim (\chi^2 a, b, \frac{1}{\chi^2}c)$$

and it finishes, so we have $m = 2l$. The number of identified cycles depends on $ord(\chi)$.

All in all, there are three types of cycles:

- Cycles with odd period where no equivalence $[(a,b,c)]_U \sim [(\mu a, b, \frac{1}{\mu}c)]_U$ occurs.
- Cycles with even period such that no equivalence of the mentioned type occurs.
- Cycles with even period such that, after half of the period, the equivalence $[(a,b,c)]_U \sim [(\mu a, b, \frac{1}{\mu}c)]_U$ comes up.

It is known that, given $q = p^n$, -1 is a square in $\mathbb{F}_q$ iff p is a prime of the form $4k+1$ and/or n is even. We can restate theorem 13.16:

Theorem 13.18. *If $-1 \in (\mathbb{F}_q^*)^2$, then the equivalence $[f]_U \sim [g]_U$ implies $[g]_U \in Cic([f]_U)$.*

On the other hand, if $-1 \notin (\mathbb{F}_q^*)^2$ and $f = (a,b,c)$, then the equivalence $[f]_U \sim [g]_U$ implies that $[g]_U \in Cic([(a,b,c)]_U)$ or $[g]_U \in Cic([(\mu a, b, \frac{1}{\mu}c)]_U)$.

As we can see, this theorem is not complete.

13.4 Cycles and Pell's equation

Now we will try to use what we know about Pell's equation. We forget about the class $[f]_U$ and use the previous objects, where $f_1, \cdots, f_m$ are the forms compounding the cycle and

$$N_{\delta_i} = \begin{pmatrix} 0 & 1 \\ -1 & \delta_i \end{pmatrix},$$

is the form which transforms f_i into f_{i+1}. We will suppose the form f_1 has principal root ω_1 and its pure periodic scf is

$$\omega_1 = [0; *\delta_1, -\delta_2 \cdots, (-1)^{m-1}\delta_m, (-1)^m\delta_1, \cdots, *\delta_m],$$

and we will work with its convergents $R_n = \frac{P_n}{Q_n}$.

Lemma 13.19. *Denoting $N_{\delta_0} = Id$, for every $k \geq 0$ the following identity holds:*

$$M_k := N_{\delta_0} \cdots N_{\delta_k} = \begin{pmatrix} (-1)^{\frac{k(k+1)}{2}} P_{k-1} & (-1)^{\frac{(k+3)(k+4)}{2}} P_k \\ (-1^{\frac{k(k+1)}{2}}) Q_{k-1} & (-1)^{\frac{(k+3)(k+4)}{2}} Q_k \end{pmatrix}.$$

Proof. The proof is identical to that in $\mathbb{Z}$, it can be done by simple calculation and applying the definitions of P_n and Q_n.

□

Proposition 13.20. *For every plant D, $Pell(D)$ contains non-trivial solutions.*

Proof. We define f_1 as the principal reduced form I_p. If $m = 1$ it means we are considering the trivial cycle, so without loss of generality we can suppose $m \geq 2$.Therefore, the transformation M_m cannot be the identity. We also know that $f_1|_{M_m} = f_1$, therefore M_m is a non-trivial automorph. Using the correspondence between automorphs and $Pell(D)$, we are done.

□

Unfortunately, since we did not control as well as in $\mathbb{Z}$ the parity of the period of the scf of the principal root we cannot deduce too much about the existence of solutions to $\mu-$Pell's equation. Just the following, which is not too powerful:

Proposition 13.21. *If $-1 \in (\mathbb{F}_q^*)^2$ and $\mu Pell(D)$ is not empty, then every cycle of forms $[f]_U$ has even period.*

Proof. Since $\mu Pell(D)$ is not empty, for every form f with such discriminant there exists a μ-morph M. Then, since -1 is a square, it implies that $[f|_M]_U \in Cic([f]_U)$. From the classification stated above, it implies the cycle has even period.

□

13.5 Summary

This is what we have done along this chapter: given a plant D, there exists a finite number of reduced forms with such discriminant. Everyone of those is

equivalent to at least one reduced form, although this definition of reduced form was not too restrictive, which, together with the fact that their behavior is slightly different, implied that the cycles we defined did not work as well as in $\mathbb{Z}$. We solved this by considering the class $[f]_U$, which actually is equivalent to doing $\operatorname{sgn} a \in \{1, a\}$.

After doing this, however, we could not completely prove that equivalence implies sharing cycle.

Finally, the actual reduced forms are the classes $[f]_U$, or equivalently their representatives satisfying $\operatorname{sgn} a \in \{1, \mu\}$. So given the set $Cl(D)$, each class has many representatives satisfying $\operatorname{sgn} a \in \{1, \mu\}$, and we just have to choose one of each class.

Chapter 14

Degenerated cases

14.1 Perfect square discriminant

Definition 14.1. *A form (a, b, c) with discriminant h^2, $h \in A$, is called* reduced *if*

$$|a| < |h|; \quad b = h; \quad c = 0, \text{ and } \operatorname{sgn} a \in \{1, \mu\}.$$

in other words if it has the form

$$(A, h, 0)$$

where $|A| < |h|$ and $\operatorname{sgn} A \in \{1, \mu\}$.

It is easy to see that the number of reduced forms with a given discriminant is finite. It is remarkable that, since primitive forms are only equivalent to primitive forms, the mentioned A is coprime to h.

Proposition 14.2. *Every class in $Cl(D)$ contains at least one reduced form.*

Proof. Suppose we are given a form (a, b, c) with square discriminant h^2. We aim to prove that there exists $(A, h, 0)$, $|A| < |h|$, $\operatorname{sgn} A \in \{1, \mu\}$ which is equivalent to the given one. Without loss of generality we can suppose (a, b, c) is half-reduced, hence a, c are not zero. This implies $b \neq \pm h$.

We define β, δ as coprime polynomials so that $\frac{\beta}{\delta} = \frac{(h-b)/2}{a}$. We can also find α, γ so that $\alpha\gamma - \beta\delta = 1$. We have

$$\frac{(h-b)/2}{a} = \frac{c}{-(h+b)/2} = \frac{\beta}{\delta},$$

so if we apply the transformation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ to (a, b, c), the resultant form (a', b', c') satisfies the following equalities:

$$b' = b(\alpha\delta + \beta\gamma) + 2(a\beta\alpha + c\delta\gamma) =$$

$$= b(\alpha\delta + \beta\gamma) + 2(\delta\tfrac{h-b}{2}\alpha - \beta\tfrac{h+b}{2}\gamma) = h(\alpha\gamma - \beta\delta) = h;$$

$$c' = a\beta^2 + b\beta\delta + c\delta^2 =$$

$$= \delta\beta\tfrac{h-b}{2} + b\beta\delta - \delta\beta\tfrac{b+h}{2} = 0.$$

Now, if $|a'| < |h|$, then we are done by normalizing and setting $A = a'$. Otherwise we define $A = a' + hk$ where k is the unique polynomial so that $|A| < |h|$ and apply $TS^{-k}T$ to the form $(a', h, 0)$ to convert it into $(A, h, 0)$. We normalize it and the proof is finished.

□

In last result, if $A = 0$ then, since $(0, h, 0)$ is primitive, we deduce $h \in \mathbb{F}_q^*$ and $D \in (\mathbb{F}_q^*)^2$. So we can assert that every form f with discriminant $|h^2| \geq 2$ has a primitive equivalent form $(A, h, 0)$ such that $0 < |A| < |h|$. Now we want to show these reduced forms are unique.

Proposition 14.3. *Every class in $Cl(D)$ contains exactly one reduced form.*

Proof. Suppose we are given equivalent reduced forms $(a, h, 0)$ and $(a', h, 0)$. We aim to show they are identical. If there exists a transformation of the usual type satisfying $\alpha\gamma - \beta\delta = 1$, then the equivalence equations 10.2 give:

1. $a' = a\alpha^2 + h\alpha\gamma$
2. $h = h(\alpha\delta + \beta\gamma) + 2a\alpha\beta$
3. $0 = a\beta^2 + h\beta\delta$

Doing $(2) \times \beta - (3) \times 2\alpha$ we arrive to

$$h\beta = -h\beta(\alpha\gamma - \beta\delta) = -h\beta,$$

therefore $\beta = 0$. Since the determinant is 1, this implies $\alpha = \psi$ and $\delta = \psi^{-1}$, where $\psi \in (\mathbb{F}_q)^*$. So (1) has the form

$$a' = \psi^2 a \pm h\gamma,$$

but this can only hold if $\gamma = 0$, for $|a| < |h|$ and $|a'| < |h|$. All in all $a = \psi^2 a'$. From $\operatorname{sgn} a \in \{1, \mu\}$ and $\operatorname{sgn} a' \in \{1, \mu\}$, we deduce the given forms are identical, as desired.

□

All in all, we have showed that $Cl(D)$ is finite and we can choose the representative of every class to be its unique reduced form.

14.2 Zero discriminant

The following proposition completely determines this case:

Proposition 14.4. *The class group $Cl(0)$ contains two elements, which are $(1, 0, 0)$ and $(\mu, 0, 0)$.*

Proof. Suppose we are given a form $f = (a, b, c)$ so that $D = b^2 - 4ac = 0$

We can write $b = 2b'$ and from $b'^2 = ac$ we deduce that there exist $a', c' \in A$ such that either $(a, c) = (a'^2, c'^2)$ or $(a, c) = (\mu a'^2, \mu c'^2)$. Note that we used that f is primitive, but also that A is an UFD. So we have

$$ax^2 + bxy + cy^2 = (Ax + Cy)^2, \text{ or } ax^2 + bxy + cy^2 = \mu(Ax + Cy)^2,$$

where A and C are coprime, which implies that there exist $\alpha, \gamma \in A$ such that $A\alpha + C\gamma = 1$. So we apply the equivalent transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & C \\ \gamma & A \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix},$$

which converts $Ax + Cy$ into x'. Hence f is equivalent to either $(1, 0, 0)$ or $(\mu, 0, 0)$, as desired.

□

Chapter 15

Composition of forms

In this chapter we aim to expose the composition of forms with coefficients in A whose discriminants coincide. However, the parallelism between the case in $\mathbb{Z}$ and the present case is so clear (including all formulas, which are identical) that writing a completely detailed explanation would seem repetitive. Therefore our demonstrations will just consist on comments about the respective propositions in $\mathbb{Z}$.

The idea that encourages the composition of two forms is to find the form representing all products of polynomials represented by these two forms. In other words, if f, f' are primitive forms of discriminant D, then a form F of the same discriminant is their composition if

$$f(x_1, y_1)f'(x_2, y_2) = F(X, Y),$$

after applying a bilinear transformation of the form

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix},$$

where $a_i, b_i, c_i, d_i \in A$.

Our way to find that transformation passes through *united* forms:

Definition 15.1. *Two forms* (a_1, b_1, c_1) *and* (a_2, b_2, c_2) *are* united *if they share discriminant and* $\gcd(a_1, a_2, b_1 + b_2) = 1$.

We have the following proposition, which can be proved by means of the same tools we use in $\mathbb{Z}$ for corollary 7.4. The only difference we should remark is the fact that our "prime numbers" are the irreducible polynomials.

Proposition 15.2. *Given $f = (a, b, c)$ and $f_1 = (a_1, b_1, c_1)$, there exists $f_2 = (a_2, b_2, c_2)$ so that $f_2 \sim f_1$ and* $\gcd(a, a_2) = 1$.

This means that united forms are wide enough to "substitute" every pair of classes in $Cl(D)$. However, united forms are not simple enough to make explicit our composition formula. We will need a subset of these pairs, the *prepared* forms. The proof of the following proposition is a copy of that in $\mathbb{Z}$.

Proposition 15.3. *If (a_1, b_1, c_1) and (a_2, b_2, c_2) are united then there exist $B, C \in A$ such that*

$$(a_1, b_1, c_1) \sim (a_1, B, a_2C)$$
$$(a_2, b_2, c_2) \sim (a_2, B, a_1C).$$

These two new forms are also united.

In order to distinguish the pair of forms $f = (a_1, B, a_2C)$ and $f' = (a_2, B, a_1C)$ from general united forms, we will say they are *prepared*. Now we are able to write the composition of these f and f', for the following equation holds:

$$(a_1{x_1}^2 + Bx_1y_1 + a_2C{y_1}^2)(a_2{x_2}^2 + Bx_2y_2 + a_1C{y_2}^2) = a_1a_2X^2 + BXY + CY^2,$$

by means of the transformation

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix}.$$

Definition 15.4. *The* compounded form *of the prepared forms $f = (a_1, B, a_2C)$ and $f' = (a_2, B, a_1C)$ is $F = (a_1a_2, B, C)$, what we denote as $F = f_1 \circ f_2$.*

Now we must go for a well-defined extension to $Cl(D)$. First we state the following lemma, whose demonstration in $\mathbb{Z}$ is perfectly adaptable (actually, we have maintained the invertible elements in the modulo in order to make it completely identical).

Lemma 15.5. *Two forms (a_1, b_1, c_1) and (a_2, b_2, c_2) of the same discriminant are equivalent if and only if there exist $\alpha, \gamma \in A$ such that*

$$a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 = a_2$$
$$2a_1\alpha + (b_1 + b_2)\gamma \equiv 0 \pmod{2a_2}$$
$$(b_1 - b_2)\alpha + 2c_1\gamma \equiv 0 \pmod{2a_2}.$$

This lemma is used for the following theorem. In this case the proof is almost identical again, but there is an important fact that should not be overlooked: $\sqrt{D}$ exists only if D is a plant, so the notation $\sqrt{D}$ should be used only in congruences.

Theorem 15.6. *Given the pairs of prepared forms*

$$f_1 = (a_1, B, a_2C), \quad f_2 = (a_2, B, a_1C)$$

$$f_3 = (m_1, N, m_2L), \quad f_4 = (m_2, N, m_1L),$$

and assuming $f_1 \sim f_3$ and $f_2 \sim f_4$, it also holds $f_1 \circ f_2 \sim f_3 \circ f_4$.

This result allows us to define a general composition. From now on, we will write $[f]$ to refer to the class of the form f.

Suppose we are given the forms f, f', which must share discriminant. Using proposition 15.2, there exists f'_u so that $f' \sim f'_u$ and the pair f, f'_u is united. Using proposition 15.3, there exist f_p and f'_p so that $f \sim f_p$, $f' \sim f'_u \sim f'_p$ satisfying that f_p and f'_p are prepared.

Then we can define

$$[f] \circ [f'] = [f_p] \circ [f'_p] := [f_p \circ f'_p],$$

where the first equality follows from the definition of class and the second one is well-defined from the last theorem.

The properties of this composition can be seen following the reasoning made in $\mathbb{Z}$. All in all, we can state the following theorem:

Theorem 15.7. *Under the defined composition, the classes of forms of a fixed discriminant form a finite abelian group. The identity of the group is the principal class, and the inverse of the class of any form is the class of the opposite of the form.*

Chapter 16

Easy class groups

Now we can expose some simple groups of classes. When writing the form (a, b, c) we will be referring to the class $[(a, b, c)]$.

Zero discriminant

In this case we have $Cl(0) = \{(1, 0, 0), (\mu, 0, 0)\}$. These forms are already prepared, so to compound them we just have to multiply the left coefficients and then normalize the resultant form. Although we could define this operations considering only the set $\{1, \mu\}$, we can also write it as

$$Cl(0) \cong (\mathbb{F}_q^* \Big/ (\mathbb{F}_q^*)^2),$$

via the isomorphism $\phi : (\psi, 0, 0) \mapsto [\psi]$, where $\psi \in \{1, \mu\}$.

Square discriminant

Given $D = h^2$, we prefer to distinguish the cases when $|h| = 1$ and $|h| > 1$.

If $|h^2| = 1$, then $h = \psi \in \mathbb{F}_q^*$. Since we must find an $|a| < |h|$, the only option is $Cl(\psi^2) = \{(0, \psi, 0)\}$. We have $(0, \psi, 0) \circ (0, \psi, 0) = (0, \psi, 0)$, so $Cl(\psi^2)$ is the trivial group.

On the other hand, if $|h^2| > 1$, firstly we define

$$\Phi(h) := \{p \in A \text{ such that } |p| < |h|,\ \gcd(h, p) = 1 \text{ and } \operatorname{sgn} p \in \{1, \mu\}\ \},$$

so we have

$$Cl(h^2) = \{(a, h, 0)\}_{a \in \Phi(h)}.$$

These forms are already prepared and again what we do to multiply them is multiplying the first coefficients and normalizing. This can be differently explained by considering the mapping

$$\begin{aligned} \phi\colon Cl(h^2) &\to {}^{(A}\!/_{hA)^*} \Big/ {}^{(\mathbb{F}_q^*}\!\Big/_{(\mathbb{F}_q^*)^2)} \\ (a,h,0) &\mapsto [a] \end{aligned}$$

which actually is an isomorphism, hence the group on the right hand side is $Cl(h^2)$.

Bibliography

[1] C. F. Gauss, *Disquisitiones Arithmeticae*, spanish translation by Hugo Barrantes, Michael Josephy and Ángel Ruiz, San José
CIMM, Universidad de Costa Rica

[2] D.A. Buell, *Binary Quadratic Forms*
Springer,1989.

[3] G.B. Mathews *The Theory of Numbers*, part 1.
Deighton Bell and Co. 1892

[4] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*
Oxfors Science Publication 2003